DEPARTMENT OF THE NAVY
NAVAL UNDERSEA WARFARE CENTER DIVISION
610 DOWELL STREET
KEYPORT, WASHINGTON 98345-7610

5720
00L/028
13 May 21

Ms. Rose Santos
FOIA Group, Inc.
P.O. Box 368
Depew, NY 14043

Subj: PARTIAL DENIAL OF FREEDOM OF INFORMATION ACT REQUEST DON-NAVY-2021-004821 FOR CONTRACT N00178-19-D-8173

Dear Ms. Santos:

This letter is in response to your Freedom of Information Act (FOIA) request dated April 12, 2019, for information pertaining to contract N00178-19-D-8173 in which you seek clearly releasable copy of the task order's title page and current statement of work/performance of statement.

Review of the requested documents reveals that they are partially exempt from disclosure under the FOIA. Exemption (b)(6) protects personal information such as names, phone numbers, and email addresses, which have been redacted accordingly.

Fees incurred during the processing of your request amount to $39.50 for .25 hours of search, and .25 hours of review. Accordingly, please forward a check or money order, payable to the Treasurer of the United States, for the stated amount, to this office within 30 calendar days from the date of this correspondence.

You have the right to an administrative appeal. It must be received within 90 calendar days from the date of this letter. Please attach a copy of your initial request and amended request, a copy of this letter, and mark the appeal letter and envelope "Freedom of Information Act Appeal." Mail your appeal to:

Department of the Navy,
Office of the General Counsel,
1000 Navy Pentagon, Room 4E635, Washington, DC
20350-1000

Please send a copy of your appeal to the Naval Undersea Warfare Center, Keyport, FOIA Coordinator, 610 Dowell Street, Keyport, WA 98345-7610. You are encouraged to provide an explanation why you believe the redactions were inappropriate or our search was inadequate.

If you have any questions, please contact the FOIA Coordinator at andrew.j.phillips1@navy.mil and (360) 396-2785. You may also contact the DON FOIA Public Liaison, Christopher Julka, at christopher.a.julka@navy.mil, (703)697-0037.

Sincerely,

R. M. JUSKO
Counsel

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 125

1. CONTRACT/PURCH ORDER/AGREEMENT NO.	2. DELIVERY ORDER/CALL NO.	3. DATE OF ORDER/CALL (YYYYMMMDD)	4. REQUISITION/PURCH REQUEST NO.	5. PRIORITY
N0017819D8173	N0025321F3001	2020NOV25	Various	DO-C9

6. ISSUED BY CODE N00253

NUWC, KEYPORT DIVISION
610 Dowell Street
Keyport, WA 98345-7610

7. ADMINISTERED BY *(If other than 6)* CODE

SCD: C

8. DELIVERY FOB
- ☐ DESTINATION
- ☐ OTHER *(See Schedule if other)*

9. CONTRACTOR CODE 1PYX5 FACILITY 135914880

NAME AND ADDRESS
Network and Simulation Technologies Inc. dba NETSIMCO
1 Corporate Place
Middletown, RI 02842

10. DELIVER TO FOB POINT BY *(Date) (YYYYMMMDD)*: SEE SCHEDULE

11. X IF BUSINESS IS
- ☒ SMALL
- ☐ SMALL DISAD-VANTAGED
- ☐ WOMEN-OWNED

12. DISCOUNT TERMS: Net 30 Days WAWF

13. MAIL INVOICES TO THE ADDRESS IN BLOCK: SEE SECTION G

14. SHIP TO CODE

SEE SECTION F

15. PAYMENT WILL BE MADE BY CODE HQ0337

DFAS Columbus Center, North Entitlement Operations
P.O. Box 182266
Columbus, OH 43218-2266

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER

- DELIVERY/CALL ☒ This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.
- PURCHASE ☐ Reference your furnish the following on terms specified herein.

ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

Network and Simulation Technologies Inc. dba NETSIMCO		(b) (6)	
NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED (YYYYMMMDD)

☐ If this box is marked, supplier must sign Acceptance and return the following number of copies:

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE

SEE SCHEDULE

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	SEE SCHEDULE				

*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.

24. UNITED STATES OF AMERICA
BY: /s/Anita Moosmiller 11/25/2020
CONTRACTING/ORDERING OFFICER

25. TOTAL $16,897,562.00

26. DIFFERENCES

27a. QUANTITY IN COLUMN 20 HAS BEEN
☐ INSPECTED ☐ RECEIVED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	c. DATE (YYYYMMMDD)	d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	28. SHIP. NO.	29. D.O. VOUCHER NO.	30. INITIALS
	☐ PARTIAL ☐ FINAL	32. PAID BY	33. AMOUNT VERIFIED CORRECT FOR
f. TELEPHONE NUMBER / g. E-MAIL ADDRESS	31. PAYMENT		34. CHECK NUMBER
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.	☐ COMPLETE ☐ PARTIAL ☐ FINAL		
a. DATE (YYYYMMMDD) / b. SIGNATURE AND TITLE OF CERTIFYING OFFICER			35. BILL OF LADING NO.

37. RECEIVED AT	38. RECEIVED BY *(Print)*	39. DATE RECEIVED (YYYYMMMDD)	40. TOTAL CONTAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

Section C - Description/Specifications/Statement of Work

NOTE 1: All clauses incorporated by reference and full text in the basic IDIQ contract apply to this Task Order, as applicable, in addition to those added here.

(End of Note)

CLAUSES INCORPORATED BY FULL TEXT

C-202-H001 ADDITIONAL DEFINITIONS--BASIC (NAVSEA) (OCT 2018)
(a) Department - means the Department of the Navy.

(b) Commander, Naval Sea Systems Command - means the Commander of the Naval Sea Systems Command of the Department of the Navy or his duly appointed successor.

(c) References to The Federal Acquisition Regulation (FAR) - All references to the FAR in this contract shall be deemed to also reference the appropriate sections of the Defense FAR Supplement (DFARS), unless clearly indicated otherwise.

(d) National Stock Numbers - Whenever the term Federal Item Identification Number and its acronym FIIN or the term Federal Stock Number and its acronym FSN appear in the contract, order or their cited specifications and standards, the terms and acronyms shall be interpreted as National Item Identification Number (NIIN) and National Stock Number (NSN) respectively which shall be defined as follows:

(1) National Item Identification Number (NIIN). The number assigned to each approved Item Identification under the Federal Cataloging Program. It consists of nine numeric characters, the first two of which are the National Codification Bureau (NCB) Code. The remaining positions consist of a seven digit non-significant number.

(2) National Stock Number (NSN). The National Stock Number (NSN) for an item of supply consists of the applicable four-position Federal Supply Class (FSC) plus the applicable nine-position NIIN assigned to the item of supply.

(End of Text)

C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)
(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained. These official files may contain information that is considered a trade secret, proprietary, business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as “protected information”. File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein.

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that:

(1) The support contractor not disclose any information;

(2) Individual employees are to be instructed by the support contractor regarding the sensitivity of the official contract files;

(3) The support contractor performing these services be barred from providing any other supplies and/or services, or competing to do so, to NAVSEA for the period of performance of its contract and for an additional three years thereafter unless otherwise provided by law or regulation; and,

(4) In addition to any other rights the contractor may have, it is a third party beneficiary who has the right of direct action against the support contractor, or any person to whom the support contractor has released or disclosed protected information, for the

unauthorized duplication, release, or disclosure of such protected information.

(c) Execution of this contract by the contractor is considered consent to NAVSEA's permitting access to any information, irrespective of restrictive markings or the nature of the information submitted, by its file room management support contractor for the limited purpose of executing its file room support contract responsibilities.

(d) NAVSEA may, without further notice, enter into contracts with other contractors for these services. Contractors should enter into separate non-disclosure agreements with the file room contractor. Contact the Procuring Contracting Officer for contractor specifics. However, any such agreement will not be considered a prerequisite before information submitted is stored in the file room or otherwise encumber the government.

(End of Text)

C-211-H017 UPDATING SPECIFICATIONS AND STANDARDS (NAVSEA) (DEC 2018)

The contractor may request that this contract be updated to include the current version of the applicable specification or standard if the update does not affect the form, fit or function of any deliverable item or increase the cost/price of the item to the Government. The contractor should submit update requests to the Procuring Contracting Officer with copies to the Administrative Contracting Officer and cognizant program office representative for approval. The contractor shall perform the contract in accordance with the existing specifications and standards until notified of approval/disapproval of its request to update by the Procuring Contracting Officer. Any approved alternate specifications or standards will be incorporated into the contract.

(End of Text)

C-211-H018 APPROVAL BY THE GOVERNMENT (NAVSEA) (JAN 2019)

Approval by the Government as required under this contract and applicable specifications shall not relieve the Contractor of its obligation to comply with the specifications and with all other requirements of the contract, nor shall it impose upon the Government any liability it would not have had in the absence of such approval.

(End of Text)

C-212-W002 COMMERCIAL SUPPLIER AGREEMENTS (NAVSEA) (MAR 2019)

(a) Commercial Supplier Agreement means End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement.

(b) Any Commercial Supplier Agreement must be provided in full text as part of a quote or offer without hyperlinks.

(c) The contract/order Schedule and Federal Acquisition Regulation (FAR) 52.212-4, Contract Terms and Conditions —Commercial Items, shall take precedence over any conflicting provisions in a Commercial Supplier Agreement.

(d) If any requirement in the Commercial Supplier Agreement conflicts with Federal law or regulations (see FAR 12.212(a)), the following shall apply:

(i) Any such requirement is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such requirement by virtue of it appearing in the Commercial Supplier Agreement. If the Commercial Supplier Agreement is invoked through an “I agree” click box or other comparable mechanism (e.g., “click-wrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such requirement.

(iii) Any such requirement is deemed to be stricken from the Commercial Supplier Agreement.

(e) Automatic renewals. License Agreements will expire at end of the term identified in the Purchase Order/Contract. Automatic renewals are not permitted and any such provision is void.

(f) Changes to the Commercial Supplier Agreement. Unilateral changes of the Commercial Supplier Agreement are impermissible and any requirement authorizing such changes is unenforceable. Changes must be in writing and executed by both parties to be effective.

(g) Third Part License (Embedded Software).

(i) The Contractor agrees that it has obtained all necessary licenses for the Government for any third party materials (including without limitation all Open Source licenses) provided within the product.

(ii) Contractor agrees that it complies with and shall continue to comply with all of its obligations under Third Party Licenses

(including without limitation all Open Source licenses) associated with any third party materials provided within each product.

(iii) To the extent that the Government's use of the software products licensed herein is in compliance with the Contractor's Commercial Supplier Agreement, the Government's use will also be in compliance with any Third Party Licenses.

(h) Audits. In lieu of any audit provisions in the Commercial Supplier Agreement, the Government agrees that, no more than once every twelve (12) months or within a reasonable time after a transfer, the Contractor shall, upon reasonable notice, have the right to require that the Government conduct an internal audit to ascertain and verify the number of licenses in use and to verify that the Government's use of the product is in conformity with this Agreement. The Government is not required to use any tools provided by the Contractor to conduct the audit and shall not be required to pay for any tools provided by the Contractor to conduct the audit. The results of any such audit shall be kept confidential.

If verification discloses that the Government's use is not in conformity with this Agreement, the Government agrees to resolve any noncompliance by either removing or correcting the unlicensed installation and use of the software identified by the audit as not in conformity with this Agreement.

(i) Confidentiality. Commercial Supplier Agreements' terms and the final contract pricing may not be deemed confidential. Other marked confidential information will be appropriately guarded.

(j) Assignment. The Government shall have the right, without the prior written consent of the Contractor or its authorized resellers, to assign, reassign, or transfer software licenses among Government employees or the Government's rights in the Contractor's product to any governmental organization that is managed, operated, or controlled by the Government.

Such authorization includes sublicensing, and assignment or transfer among or between authorized users. In the event authorized users are reorganized or restructured such that their responsibilities and operations are transferred to another government agency, the agency shall have the right to assign the affected program licenses to a successor agency. The licensed agency and the successor agency agree to be bound to the Commercial Supplier Agreement as modified. The transferee shall be bound by the license metrics and limitations in this license. Government shall complete any documentation required by the Contractor to facilitate the transfer of this license, and continuation of support shall be the responsibility of the transferee.

For the avoidance of doubt, any assignment or transfer of licenses of the Contractor's products is also subject to all other terms of the Commercial Supplier Agreement, as well as the Contractor's policies governing product dependencies and version compatibility. Reassignment does not require that the license be under maintenance or support in order to execute a transfer.

(k) Litigation. Any requirement insisting that the commercial supplier or licensor control any litigation arising from the government's use of the contractor's supplies or services is deleted and unenforceable.

(l) Equitable Remedies. Equitable remedies, injunctive relief, and binding arbitration requirements shall not be enforced unless explicitly authorized by agency guidance or statute.

(m) Venue. Any claim or dispute shall be resolved under the Contract Disputes Act and FAR 52.233-1. The forum for resolution of disputes and applicable statutes of limitation shall be governed by federal law.

(n) Applicable law. In accordance with FAR 52.233-4, United States law shall apply to resolve any claim of breach of this contract and such actions shall be handled in the applicable Federal court of jurisdiction.

(End of Text)

C-215-H002 CONTRACTOR PROPOSAL (NAVSEA) (OCT 2018)

(a) Performance of this contract by the Contractor shall be conducted and performed in accordance with detailed obligations to which the Contractor committed itself in Proposal N0025320R3000 dated 20 March 2020 in response to NAVSEA Solicitation No. N0025320R3000. .

(b) The technical volume(s) of the Contractor's proposal is(are) hereby incorporated by reference and made subject to the "Order of Precedence" (FAR 52.215-8) clause of this contract. Under the "Order of Precedence" clause, the technical volume(s) of the Contractor's proposal referenced herein is (are) hereby designated as item (f) of the clause, following "the specifications" in the order of precedence.

(End of Text)

C-223-W002 ON-SITE SAFETY REQUIREMENTS (NAVSEA) (OCT 2018)

(a) The contractor shall ensure that each contractor employee reads any necessary safety documents within 30 days of commencing performance at any Government facility. Required safety documents can be obtained from the respective safety office. Contractors shall notify the Safety office points of contact below to report completion of the required training via email. The email shall include the contractor employee's name, work site, and contract number.

(b) It is expected that contractor employees will have received training from their employer on hazards associated with the areas in

which they will be working and know what to do in order to protect themselves. Contractors are required to adhere to the requirements of 29 CFR 1910, 29 CFR 1926 and applicable state and local requirements while in Government spaces. The contractor shall ensure that all on-site contractor work at the Government facility is in accordance with any local safety instructions as provided via the COR. The contractor shall report all work-related injuries/illnesses that occurred while working at the Government site to the COR.

(c) Contractors whose employees perform work within Government spaces in excess of 1000 hours per calendar quarter during a calendar year shall submit the data elements on OSHA Form 300A, Summary of Work Related Injuries and Illnesses, for those employees to the safety office, via the COR by 15 January for the previous calendar year, even if no work related injuries or illnesses occurred. If a contractor's injury/illness rates are above the Bureau of Labor Statistics industry standards, a safety assessment may be performed by the Safety Office to determine if any administrative or engineering controls can be utilized to prevent further injuries/illnesses, or if any additional Personal Protective Equipment or training will be required.

(d) Any contractor employee exhibiting unsafe behavior may be removed from the Government site. Such removal shall not relieve the contractor from meeting its contractual obligations and shall not be considered an excusable delay as defined in FAR 52.249-14.

(e) The Safety Office points of contacts are as follows:

To be provided by COR after award.

(End of Text)

C-227-H006 DATA REQUIREMENTS (NAVSEA) (OCT 2018)
The data to be furnished hereunder shall be prepared in accordance with the Contract Data Requirements List, DD Form 1423, Exhibit(s) A, attached hereto.

(End of Text)

C-227-H008 GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM (NAVSEA) (DEC 2018)
(a) The contractor shall actively participate in the Government Industry Data Exchange Program in accordance with the GIDEP Operations Manual, S0300-BT-PRO-010. The contractor shall submit information concerning critical or major nonconformances, as defined in FAR 46.407/DFARS 246.407, to the GIDEP information system.

(b) The contractor shall insert paragraph (a) of this clause in any subcontract when deemed necessary. When so inserted, the word "contractor" shall be changed to "subcontractor."

(c) The contractor shall, when it elects not to insert paragraph (a) in a subcontract, provide the subcontractor any GIDEP data which may be pertinent to items of its manufacture and verify that the subcontractor utilizes any such data.

(d) The contractor shall, whether it elects to insert paragraph (a) in a subcontract or not, verify that the subcontractor utilizes and provides feedback on any GIDEP data that may be pertinent to items of its manufacture."

(e) GIDEP materials, software and information are available without charge from:

GIDEP Operations Center

P.O. Box 8000
Corona, CA 92878-8000
Phone: (951) 898-3207
FAX: (951) 898-3250
Internet: http://www.gidep.org

(End of Text)

C-227-H009 ACCESS TO DATA OR COMPUTER SOFTWARE WITH RESTRICTIVE MARKINGS (NAVSEA) (JAN 2019)

(a) Performance under this contract may require that the Contractor have access to technical data, computer software, or other sensitive data of another party that contains restrictive markings. If access to such data or software is required or to be provided, the Contractor shall enter into a written agreement with such party prior to gaining access to such data or software. The agreement shall address, at a minimum, (1) access to, and use of, the restrictively marked data or software exclusively for the purposes of performance of the work required by this contract, and (2) safeguards to protect such data or software from unauthorized use or disclosure for so long as the data or software remains properly restrictively marked. In addition, the agreement shall not impose any limitation upon the Government or its employees with respect to such data or software. A copy of the executed agreement shall be provided to the Contracting Officer. The Government may unilaterally modify the contract to list those third parties with which the Contractor has agreement(s).

(b) The Contractor agrees to: (1) indoctrinate its personnel who will have access to the data or software as to the restrictions under which access is granted; (2) not disclose the data or software to another party or other Contractor personnel except as authorized by the Contracting Officer; (3) not engage in any other action, venture, or employment wherein this information will be used, other than under this contract, in any manner inconsistent with this requirement; (4) not disclose the data or software to any other party, including, but not limited to, joint venturer, affiliate, successor, or assign of the Contractor; and (5) reproduce the restrictive stamp, marking, or legend on each use of the data or software whether in whole or in part.

(c) These restrictions on use and disclosure of the data and software also apply to information received from the Government through any means to which the Contractor has access in the performance of this contract that contains restrictive markings.

(d) The Contractor agrees that it will promptly notify the Contracting Officer of any attempt to gain access to any information with restrictive markings. Such notification shall include the name and organization of the individual, company, or Government representative seeking access to such information.

(e) The Contractor shall include this requirement in subcontracts of any tier which involve access to information covered by paragraph (a), substituting "subcontractor" for "Contractor" where appropriate.

(f) Compliance with this requirement is a material requirement of this contract.

(End of Text)

C-227-H010 COMPUTER SOFTWARE AND COMPUTER DATA BASES DELIVERED TO OR RECEIVED FROM THE GOVERNMENT (NAVSEA) (JAN 2019)

(a) The Contractor agrees to test for viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4, in all computer software and computer data bases (as defined in the clause entitled “Rights In Noncommercial Computer Software and Noncommercial Computer Software Documentation” (DFARS 252.227-7014)), before delivery of that computer software or computer data base in whatever media and on whatever system the computer software or data base is delivered whether delivered separately or imbedded within delivered equipment. The Contractor warrants that when delivered any such computer software and computer data base shall be free of viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1.

(b) The Contractor agrees that prior to use under this contract, it shall test any computer software and computer data base received from the Government for viruses, malware, Trojan Horses, and other security threats listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4.

(c) Any license agreement governing the use of any computer software or computer software documentation delivered to the Government as a result of this contract must be paid-up, irrevocable, world-wide, royalty-free, perpetual and flexible (user licenses transferable among Government employees and personnel under Government contract).

(d) The Contractor shall not include or permit to be included any routine to enable the contractor or its subcontractor(s) or vendor(s) to disable the computer software or computer data base after delivery to the Government.

(e) No copy protection devices or systems shall be used in any computer software or computer data base delivered under this contract with unlimited or Government purpose rights (as defined in DFARS 252.227-7013 and 252.227-7014) to restrict or limit the Government from making copies.

(f) It is agreed that, to the extent that any technical or other data is computer software by virtue of its delivery in digital form, the Government shall be licensed to use that digital-form data with exactly the same rights and limitations as if the data had been delivered as hard copy.

(g) Any limited rights legends or other allowed legends placed by a Contractor on technical data or other data delivered in digital form shall be digitally included on the same media as the digital-form data and must be associated with the corresponding digital-form technical data to which the legend(s) apply to the extent possible. Such legends shall also be placed in human-readable form on a visible surface of the media carrying the digital-form data as delivered, to the extent possible.

(End of Text)

C-237-H001 ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (NAVSEA) (OCT 2018)

(a) The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for NUWC Keyport via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;

(2) X, Lease/Rental of Facilities;

(3) Y, Construction of Structures and Facilities;

(4) D, Automatic Data Processing and Telecommunications, IT and Telecom- Telecommunications Transmission (D304) and Internet (D322) ONLY;

(5) S, Utilities ONLY;

(6) V, Freight and Shipping ONLY.

(b) The contractor is required to completely fill in all required data fields using the following web address https://www.ecmra.mil.

(c) Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://dod.ecmra.support.desk@mail.mil.

(End of Text)

C-237-H002 SUBSTITUTION OF KEY PERSONNEL (NAVSEA) (OCT 2018)

(a) The Contractor agrees that a partial basis for award of this contract is the list of key personnel proposed. Accordingly, the Contractor agrees to assign to this contract those key persons whose resumes were submitted with the proposal necessary to fulfill the requirements of the contract. No substitution shall be made without prior notification to and concurrence of the Contracting Officer in accordance with this requirement. Substitution shall include, but not be limited to, subdividing hours of any key personnel and assigning or allocating those hours to another individual not approved as key personnel.

(b) All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The Contracting Officer shall be notified in writing of any proposed substitution at least forty-five (45) days, or ninety (90) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include: (1) an explanation of the circumstances necessitating the substitution; (2) a complete resume of the proposed substitute; (3) an explanation as to why the proposed substitute is considered to have equal or better qualifications than the person being replaced; (4) payroll record of the proposed replacement; and (5) any other information requested by the Contracting Officer to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

(c) Key personnel are identified in an attachment in Section C.

(End of Text)

C-237-W001 ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (eCRAFT) SYSTEM REPORTING (NAVSEA) (MAY 2019)

(a) The Contractor agrees to upload the Contractor's Funds and Man-hour Expenditure Reports in the Electronic Cost Reporting

and Financial Tracking (eCRAFT) System and submit the Contractor's Performance Report on the day and for the same timeframe the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination.

(b) The Contract Status Report indicates the progress of work and the status of the program and of all assigned tasks. It informs the Government of existing or potential problem areas.

(c) The Contractor's Fund and Man-hour Expenditure Report reports contractor expenditures for labor, materials, travel, subcontractor usage, and other contract charges.

(1) Access: : eCRAFT: Reports are uploaded through the eCRAFT System Periodic Report Utility (EPRU). The EPRU spreadsheet and user manual can be obtained at: http://www.navsea.navy.mil/Home/Warfare-Centers/NUWC-Newport /Partnerships/Commercial-Contracts/Information-eCraft-/ under eCRAFT information. The link for eCRAFT report submission is: https://www.pdrep.csd.disa.mil/pdrep_files/other/ecraft.htm. If you have problems uploading reports, please see the Frequently Asked Questions at the site address above.

(2) Submission and Acceptance/Rejection: Submission and Acceptance/Rejection: The contractor shall submit their reports on the same day and for the same timeframe the contractor submits an invoice in WAWF. The amounts shall be the same. eCRAFT acceptance/rejection will be indicated by e-mail notification from eCRAFT.

(End of Text)

C-242-H001 EXPEDITING CONTRACT CLOSEOUT (NAVSEA) (OCT 2018)
(a) As part of the negotiated fixed price or total estimated amount of this contract, both the Government and the Contractor have agreed to waive any entitlement that otherwise might accrue to either party in any residual dollar amount of $1,000 or less at the time of final contract closeout. The term "residual dollar amount" shall include all money that would otherwise be owed to either party at the end of the contract, except that, amounts connected in any way with taxation, allegations of fraud and/or antitrust violations shall be excluded. For purposes of determining residual dollar amounts, offsets of money owed by one party against money that would otherwise be paid by that party may be considered to the extent permitted by law.

(b) This agreement to waive entitlement to residual dollar amounts has been considered by both parties. It is agreed that the administrative costs for either party associated with collecting such small dollar amounts could exceed the amount to be recovered.

(End of Text)

C-242-H002 POST AWARD MEETING (NAVSEA) (OCT 2018)
(a) A post-award meeting with the successful offeror will be conducted within [10] days after award of the [contract / task order]. The meeting will be held at the address below:

Location/Address: NUWC Division Keyport, Keyport, WA

(b) The contractor will be given [5] working days notice prior to the date of the meeting by the Contracting Officer.

(c) The requirement for a post-award meeting shall in no event constitute grounds for excusable delay by the contractor in performance of any provisions in the [contract / task order].

(d) The post-award meeting will include, but is not limited to, the establishment of work level points of contact, determining the administration strategy, roles and responsibilities, and ensure prompt payment and close out. Specific topics shall be mutually agreed to prior to the meeting.

(End of Text)

C-242-H003 TECHNICAL INSTRUCTIONS (NAVSEA) (OCT 2018)
(a) Performance of the work hereunder may be subject to written technical instructions signed by the Contracting Officer and the Contracting Officer's Representative specified in Section G of this contract. As used herein, technical instructions are defined to

include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of drawings, specifications or technical portions of work description.

(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "CHANGES" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.

(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.

(d) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

(End of Text)

C-244-H002 SUBCONTRACTORS/CONSULTANTS (NAVSEA) (OCT 2018)

Notwithstanding FAR 52.244-2(d) and in addition to the information required by FAR 52.244-2(e) of the contract, the contractor shall include the following information in requests to add subcontractors or consultants during performance, regardless of subcontract type or pricing arrangement:

(1) Impact on subcontracting goals,

(2) Impact on providing support at the contracted value,

(3) IF SEAPORT TASK ORDER - The results of negotiations to incorporate fee rate caps no higher than the lower of (i) SeaPort-e fee rate caps for the prime contractor, or in the case where the proposed subcontractor is also a SeaPort-e prime, (ii) fee rate caps that are no higher than the subcontractor's prime SeaPort-e contract.

(End of Text)

C-245-H003 FACILITIES TO BE GOVERNMENT FURNISHED--ALTERNATE I (NAVSEA) (MAR 2019)

(a) The price and delivery schedule set forth in this contract contemplate the rent-free use of the facilities identified in paragraph (b) below. If the Government limits or terminates the Contractor's rent-free use of said facilities, and such action affects the ability of the Contractor to perform this contract in accordance with its terms and conditions, then an equitable adjustment in the price or delivery schedule or both, shall be made pursuant to the clause entitled "Changes--Fixed Price" (FAR 52.243-1) or "Changes--Cost-Reimbursement" (FAR 52.243-2), as applicable, provided; however, that if the limitation or termination is due to failure by the Contractor to perform its obligations under this contract, the Contractor shall be entitled only to such adjustment as the Contracting Officer determines to be appropriate under the circumstances.

(b) The Contractor is authorized to use the facilities described below upon the prior written approval of the cognizant Contract Administration Office, which shall determine that such facilities are required to carry out the work provided for by this contract. Immediately upon receipt of each item of approved facilities, the Contractor shall notify the cognizant Contract Administration Office of the receipt of such facilities owned by the Government, which shall be made a part of the plant account assigned to the Contractor at that location.

DESCRIPTION AND IDENTITY OF FACILITIES

Office space at NUWC Keyport

(c) In the event there is in existence a facilities management contract effective at the same plant or general location, the facilities

provided hereunder shall be made subject to all the terms and conditions of the facilities management contract.

(End of Text)

C-245-H005 INFORMATION AND DATA FURNISHED BY THE GOVERNMENT--ALTERNATE I (NAVSEA) (MAY 2019)

(a) Contract Specifications, Drawings and Data. The Government will furnish, if not included as an attachment to the contract, any unique contract specifications or other design or alteration data cited or referenced in Section C.

(b) Government Furnished Information (GFI). GFI is defined as that information essential for the installation, test, operation, and interface support of all Government Furnished Material identified in an attachment in Section J. The Government shall furnish only the GFI identified in an attachment in Section J. The GFI furnished to the contractor need not be in any particular format. Further, the Government reserves the right to revise the listing of GFI as follows:

(1) The Contracting Officer may at any time by written order:

(i) delete, supersede, or revise, in whole or in part, data identified in an attachment in Section J; or

(ii) add items of data or information to the attachment identified in Section J; or

(iii) establish or revise due dates for items of data or information in the attachment identified in Section J.

(2) If any action taken by the Contracting Officer pursuant to subparagraph (1) immediately above causes an increase or decrease in the costs of, or the time required for, performance of any part of the work under this contract, the contractor may be entitled to an equitable adjustment in the contract amount and delivery schedule in accordance with the procedures provided for in the "CHANGES" clause of this contract.

(c) Except for the Government information and data specified by paragraphs (a) and (b) above, the Government will not be obligated to furnish the Contractor any specification, standard, drawing, technical documentation, or other publication, notwithstanding anything to the contrary in the contract specifications, the GFI identified in an attachment in Section J, the clause of this contract entitled "Government Property" (FAR 52.245-1) or "Government Property Installation Operation Services" (FAR 52.245-2), as applicable, or any other term or condition of this contract. Such referenced documentation may be obtained:

(1) From the ASSIST database via the internet at https://assist.dla.mil/online/start/; or

(2) By submitting a request to the

Department of Defense Single Stock Point (DoDSSP)

Building 4, Section D
700 Robbins Avenue
Philadelphia, Pennsylvania 19111-5094
Telephone (215) 697-6396
Facsimile (215) 697-9398

Commercial specifications and standards, which may be referenced in the contract specification or any sub-tier specification or standard, are not available from Government sources and should be obtained from the publishers.

(End of Text)

PERFORMANCE WORK STATEMENT (PWS)

SECTIONS

1 - Introduction

2 - Description of Services

3 - General Information

4 - Basis of Estimate

5 - Reporting Requirements

6 - Government Furnished Property

1.0 INTRODUCTION

1.1 Background

The Naval Undersea Warfare Center Division, Keyport, WA (NUWC Keyport) In-Service Engineering (ISE) Department is responsible for life-cycle system support, including the development, maintenance and/or support of a variety of In-Service Engineering tactical and non-tactical systems. The Information Technology Division is responsible for the delivery of Navy Marine Corp Internet services and the operation of Corporate Information Technology (IT) infrastructures and applications supporting business operations and Research, Development, Test, and Evaluation (RDT&E) activities.

1.2 Purpose

1.2.1 Program Based Services

Obtain technical services in the development and system life-cycle support through system development, software application development, software modification, software support, software testing, system integration, cyber security, and systems administration. Services provided under this task order will be performed as part of a government/contractor Software Application Development and Support Team. The services provided under this task order will apply to a number of existing programs and projects, as well as similar programs, projects or work efforts that may arise or require contractor support. Each of these may have their own funding sources and Government staffing and management teams. They will be sponsored by a variety of Program Offices. NUWC Keyport has identified requirements for engineering and technical support, including functional expansion and implementation support, in the following areas, or similar systems:

- Aircraft Carrier Tactical Support Center (CV-TSC)
- Advanced Skills Management (ASM)
- Countermeasures Set Acoustic (CSA) and Tactical Decision Aid (TacDA)
- Obsolescence Management Information System (OMIS)
- Nosis/Ship to Shore Data Exchange (S2DE)
- Range Systems and Fleet Training Technology
- Fleet Test and Training Targets
- Unmanned Undersea Vehicle (UUV) Operations, Training, and Test Infrastructure
- Emergent Test and Fleet Training Infrastructure
- Weapon Systems Information Technology (WSIT)
- Augmented Reality/Virtual Reality (AR/VR)
- Cyber Security Engineering

1.2.2 Corporate Based Services

Obtain Information Technology services for the operation, maintenance, and modernization of Keyport IT infrastructures. Tasking includes:

- Unclassified and Classified Network Operations
- Corporate Voice over Internet Protocol (VoIP) Operation and Support
- IT Support Services (Tier 2 support services)
- Video Teleconference Support
- Hardware/Software Management
- Telecommunication Management
- IT Configuration Management
- Web development and modernization

- System Administration
- IT Asset Management
- Drafting Support

1.3 Scope
The contractor shall perform the tasks required and delineated in this Performance Work Statement (PWS) upon receipt of Technical Instructions (TI) from the Contracting Officer's Representative (COR).

1.4 Location of the Work
The contractor shall perform the services outlined in this work statement at NUWC Keyport, Keyport Bangor Annex, Keyport Bangor Docks and Keyport Naval Undersea Museum. Travel may be required to support tasking or initiatives at NUWC Keyport Detachments including, Hawaii, San Diego, range locations at Zelatched Point, WA, Nanaimo, Canada, and Port Angeles, WA. Additional work locations and travel may be required, but none are known at this time.

1.5 Deliverables and Digital Data Management
The Government shall own all software and data created under this task order that is not integral to the pre-existing Commercial Off-The-Shelf (COTS) software to which it relates. The contractor shall identify all software and other data to be delivered with less than Unlimited Rights. The Government reserves the right to review all data associated with and developed for this task order. The contractor shall be responsible for the digital generation, reception and electronic delivery of data. All data shall be developed, managed, used, and exchanged electronically to the greatest extent practicable. The contractor shall maintain compatibility with the World Wide Web (WWW) browser, electronic mail (e-mail), and software used by NUWC Keyport throughout the life of the task order. NUWC Keyport is on Navy Marine Corps Internet (NMCI) and runs Microsoft Office products and Adobe Acrobat. Controlled Unclassified Information (CUI) as defined in DD254, Attachment 02, transmitted via email must be encrypted to the current Department of Defense (DoD/Department of Navy (DON) standard employing Public Key Infrastructure (PKI) credentials.

1.5.1 Electronic Transmission from External (Non-Navy) Systems and Networks
Submittals requiring review shall have an electronic comment form attached. Alternatives to electronic deliveries include (but are not limited to) CD/DVD deliveries as may be directed in a TI or elsewhere in this PWS.

1.5.2 Classified Data Transmission
Classified data shall not be transmitted electronically on unclassified networks.

1.5.3 Delivery
Items submitted electronically shall be considered delivered when they are successfully transmitted and received. Items not delivered electronically shall be delivered using best commercial practice.

1.5.4 Electronic Mail
E-mail shall be used to facilitate the transfer of unclassified data only. Use of e-mail shall not relieve the contractor from compliance with other areas of this task order requiring other types of communication. No communication via e-mail can change the scope of this task order other than directly from the Contracting Officer.

1.5.5 Industry Standards

Software development and maintenance work under this task order is to be accomplished in accordance with existing and accepted industry standards. The industry standards that are applicable to this task order are:

- Software Engineering Institute - Capability Maturity Model Integrated Software Engineering Institute – Capability Maturity Model Integration (SEI-CMMI) Level 2 or higher: Version 1.3 (available online)

- Institute of Electrical and Electronics Engineers (IEEE) Standard 12207-2008 - Systems and software engineering -- Software life cycle processes: Version 2008 (available online)

1.5.6 Contract Data Requirements List Items
Contract Data Requirements List (CDRL) items are specified in Contract Exhibit A. Whenever a CDRL requirement is referenced in this PWS, the CDRL number is provided.

2.0 DESCRIPTION OF SERVICES

Most of the services in this section will be performed by contractor personnel as part of a government/contractor Software Application Development and Support Team most often using Agile methods for team and work management. The technical direction of products; prioritization of work efforts; and design, functionality and system engineering decisions are inherently governmental functions and will be made by government personnel.

The contractor shall provide necessary personnel to accomplish all contract work and services within the government specified timeframes. The contractor shall provide personnel with qualifications, necessary licenses, certifications, training, experience levels and security clearances that are required, including those required by Federal, State and local laws and regulations. Minimum requirements are identified in Table 2-1 below. Contractors must have the ability to effectively communicate (both verbally and written) to all applicable parties. Personnel assigned to these tasks will need the tact and diplomacy to effectively work with civilian and military personnel to maintain the professionalism of NUWC Division Keyport.

It is not the government's responsibility to develop private contractor employees. In the event that a one-time training event is required, or training specific to the government that cannot be obtained commercially is required, the Contracting Officer will approve the training by issuing a TI to the contractor. If it is in the Government's interest to pay for commercially available training, it may do so by issuing a TI to the contractor. The Government will not pay for any training necessary to meet the required training, education, and experience qualifications listed in Table 2-1.

2.1 Labor Categories

The following labor categories are the anticipated support; however, additional labor categories may be added after award for requirements that fall within the scope of this task order but not anticipated at this time:

2.1.1 Software (Computer) Engineering

Conduct or participate in multidisciplinary research and collaboration with equipment designers and/or hardware engineers in the planning, design, development, and utilization of electronic data processing systems software. Analyze computer user needs; advise hardware designers on machine characteristics that affect software systems such as storage capacity, processing speed, and input/output requirements; design and develop compilers and assemblers, utility programs, and operating systems. Build and code applications and/or modules. Develop patches and upgrades to existing systems.

2.1.2 & 2.1.3 Applications Software Programming (Journeyman) – JAVA, JEE, Java Script

Build and/or modify complex application programs from design specifications. Design, code, test, debug, document and maintain programs.

2.1.4 Applications Software Programming (Entry Level) – JAVA, JEE, Java Script

Build and/or modify complex application programs from design specifications. Design, code, test, debug, document and maintain programs.

2.1.5 Applications Software Programming – C#, SQL, ASP .Net

Build and/or modify complex application programs from design specifications. Design, code, test, debug, document and maintain programs.

2.1.6 Applications Software Programming – VB.Net, SQL, ASP .Net

Build and/or modify complex application programs from design specifications. Design, code, test, debug, document and maintain programs.

2.1.7 & 2.1.8 Applications Software Programming – General

Build and/or modify complex application programs from design specifications. Design, code, test, debug, document and maintain programs.

2.1.9 Applications Software Programmer (Journeyman) – C#, SQL, .Net Core

Build and/or modify complex application programs from design specifications. Design, code, test, debug, document and maintain programs.

2.1.10 Automated Test Software Programming

Build and/or modify automated test programs from test requirements, test specifications or existing software test cases as required. Design, code, test, debug, document, and integrate with open source automated test applications.

2.1.11 Test System Software Programming
Build and/or modify various test system programs from design hardware test requirements, test specifications or existing software test programs as required. Design, code, test, debug, document, integrate with associated test system hardware and maintain programs.

2.1.12 Business Analysis
Analyze, compile and document requirements for new or modified software application functionality; represent user needs to the technical development team. Create Use Cases and review development and production software for correct functionality. Document issues and desired changes in technical detail sufficient for programmers to create or modify application code, schema, database structures, screen layouts, workflow, etc.

2.1.13 Unity AR/VR Development – Mixed Reality Software Engineer
Develop, update, test, and maintain object-oriented Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) software applications for multiple hardware and software platforms using Unity game engine.

2.1.14 3D Artist Virtual Reality
Create, update, test, and maintain 3D models, Computer Aided Design (CAD), textures, materials, shaders, and sounds to build cohesive and immersive Virtual Reality (VR) environments for multiple hardware and software platforms using Unity game engine.

2.1.15 & 2.1.16 Software Test Engineering
Develop test scenarios, test cases, and test procedures for requirements compliance. Define and configure test fixtures and instrumentation. Conduct software testing; documenting defects in the defect tracking systems. Operate a variety of computer automated and manual test equipment including system simulators and stimulators. Ensure the accuracy and consistency of test data results through thorough documentation processes.

2.1.17 & 2.1.18 Software Testing
Conduct software testing and document defects in the defect tracking systems.

2.1.19 General Database Administration
Create and maintain development, test, and production databases including primary storage structures and objects. Perform capacity planning, database tuning and optimization, system resource planning and allocation, and implementation of backup and recovery strategies. Control and monitor user access to the database. Implement and enforce appropriate security protocols in accordance with Department of Defense (DoD) standards. Provide technical support to application development teams. Perform evaluation and implementation of new database technologies. Troubleshoot and resolve issues with availability, performance, and integrity of the databases.

2.1.20 General Database Administration
Create and maintain, development, test, and production databases including primary storage structures and objects. Perform capacity planning, database tuning and optimization, system resource planning and allocation, and implementation of backup and recovery strategies. Control and monitor user access to the database. Implement and enforce appropriate security protocols in accordance with DoD standards. Implement Information Assurance & Vulnerabilities Assessments (IAVA) and Security Technical Implementation Guides (STIG) as required. Provide technical support to application development teams. Perform evaluation and implementation of new database technologies. Troubleshoot and resolve issues with availability, performance, and integrity of the databases.

2.1.21 ORACLE Database Administration
Create and maintain, development, test, and production ORACLE databases including primary storage structures and objects. Perform capacity planning, database tuning and optimization, system resource planning and allocation, and implementation of backup and recovery strategies. Control and monitor user access to the database. Implement and enforce appropriate security protocols and ensure security patch levels are up to date in accordance with DoD standards. Implement IAVA and STIGs as required. Provide technical support to application development teams. Perform evaluation and implementation of new database technologies. Troubleshoot and resolve issues with availability, performance, and integrity of the databases.

2.1.22 System Administration

Perform system administration functions including maintaining hardware, ensuring operating systems, application software, and security patch levels are up to date. Monitor Windows automated update service and apply manual updates when needed. Maintain system configuration documents. Maintain network integrity and connectivity, ensure compliance with information security policies and maintain system backup and recovery capability. Perform operating system builds and rebuilds. Review IAVA and STIGs for supported operating systems and implement as required. Ensure compliance by using mandated and government-provided automated scanning tools, and provide mitigations as applicable. Document system configuration and create images utilizing various tools.

2.1.23 – 2.1.24 System Administration

Perform system administration functions. Maintain network integrity and connectivity, ensure compliance with information security policies and maintain system backup and recovery capability. Review IAVA and STIG for supported operating systems, implement and verify the implementation of the fixes. Ensure compliance by using mandated and government-provided automated scanning tools, and provide mitigations as applicable. Document system configuration and create images utilizing various tools.

2.1.25 User Interface Design

Design and develop user interfaces to support the organizations; work with multiple customer's/end users. Define, document, and implement requirements.

2.1.26 Application Support

Provide middle tier (Level 2) application support. Troubleshoot and identify issues in software applications and data housed in production, development and test databases. Document support requests in automated tracking systems and defect tracking systems.

2.1.27 IT Technical Writing

Write technical articles, reports, brochures, help files, and/or manuals for documentation for a wide range of uses. Coordinate the display of graphics and the production of the document. Work with internal teams to understand product documentation requirements. Create strong content that fulfills Navy and DoD standards. Write straight-forward user tutorials and interface text. Utilize a variety of media forms. Include images and charts. Analyze current content and make improvements as necessary.

2.1.28 – 2.1.30 Cyber Security Support Analysis

Perform Information Assurance (IA) functions for various programs and projects; these include preparing system accreditation documentation required by the Navy and/or DoD, evaluating security configurations of systems, and maintaining security configurations of production, development and test systems by applying and configuring security controls. Review IAVA and STIGs for supported operating systems, implement and verify the implementation of the STIG. Verify Cybersecurity compliance of the systems in accordance with DoD provided tools.

2.1.31 Cyber Security Support Analysis

The contractor shall provide numerous aspects of Cybersecurity Support representing Command interests and reporting as well as significant direct support to system owners and end-users. These areas include various aspects of Cybersecurity (CS) compliance and CS customer support areas. Support areas addressed by this section include oversight, support, and validation for information systems Assess and Authorize efforts; oversight of system and data access approvals, providing CS technical support and guidance developing CS policy implementation plans; IAVM/Vulnerability Remediation Asset Management execution and reporting; Communication tasking orders compliance; ensuring Command CS defense-in-depth strategy, compliance, and investigating misuse of critical IT; the Cybersecurity Workforce (CSWF) Program , ensuring compliance with Navy Cyber Defense Operations Command directives.

2.1.32 Cyber Operations Engineering

Perform advanced vulnerability assessment and analysis of systems and applications during all phases of the system life cycle. This includes: analyze developed and procured software code for security vulnerabilities; conduct penetration testing of software and evaluate security programs; perform information operations support, including cyber security engineering for applications and systems and the review and evaluation of cyber security related policies, practices and procedures.

2.1.33 Network Architect

Provide technical support in the installation, maintenance, operation, troubleshooting, upgrading and re-configuration of Keyport's

corporate network cable facilities which include unclassified, classified (Secret) environments and Sensitive Compartmented Information Facility (SCIFs). Requires Top Secret Clearance.

2.1.34 Network Administrator (VoIP Support)

Provide holistic operation of Keyport's corporate VoIP system to include maintenance, troubleshoot, design and upgrade, and re-configuration ensuring compliance with Joint Interoperability Test Command (JITC) unified communications directives, DoD policy and mandates, and Defense Information Systems Agency STIGs.

2.1.35/36/37 Computer User Support Specialist (Tier 2 level IT Support)

Operate and monitor on-site Tier 2 IT Support operations. Advocate for the customer through ticket resolution and closure for all escalated tickets. Provide analytical and technical on-site support for the operations of desktop/laptop computers, workstations, and peripherals on corporate hardware within unclassified and classified environments. Design, develop, and maintain installations of a variety of client operating systems including, but not limited to activities associated with the investigation of new operating systems, deployment and installation techniques and options, the maintenance and updates for new and existing operating systems, the configuration of the many different components of the workstation operating system to provide for reliable and stable integration into the Keyport environment

Assist the Assistant Contract Technical Representative (ACTR) in the ordering, delivery, and troubleshooting of Next Generation Enterprise Network/ Navy Marine Corps Intranet (NGEN/NMCI) services including user accounts, computers, software, and peripherals.

Manage and schedule the daily operation of Keyport's corporate Video Teleconferencing systems, that are composed of Keyport owned and NMCI systems. Schedule, setup, and troubleshoot unclassified and classified corporate Video Teleconferencing (VTC) sessions. Maintain VTC room access and usage logs. Provide monthly metrics on VTC's total number of sessions including successful and unsuccessful events

Support IT asset management activities in accordance with applicable Intelligence Community (IC) and DoD policies, instructions and guidance. Perform IT asset management activities to support the processes of inventory, IT receiving, re-use, and disposal.

2.1.38 Computer Operators (Hardware/Software Management Support)

Work with various Keyport customers on IT procurement actions, process IT Procurement Requests (ITPRs) submissions, DoN Applications and Database Management System (DADMS) new adds, associations, and updates. Track hardware and software licensing and associated maintenance renewals.

2.1.39 Telecommunications Equipment Installer

Telecommunications Management consists of the operation, ordering, delivery, and cancellation of data circuits, voice circuits, and cellular services. Must have familiarity with the Defense Information System Agency (DISA) Direct Order Entry Process. Responsible for maintaining accurate accounting of all Keyport data circuits. Provide monthly metrics on cellular usage to include under-utilization, over-utilization, and zero usage.

2.1.40 Computer Systems Analyst (IT Configuration Manager)

Responsible for developing and managing an IT Configuration Management (CM) program. Will coordinate with change initiator and Configuration Control Board (CCB) for the routing and approval of IT system changes for corporate IT systems and approved RDT&E lab capabilities.

2.1.41/42 Web Developer

The contractor shall provide the following web support utilizing such software as Microsoft Office, Hyper Text Markup Language (HTML), Microsoft SharePoint Designer, Microsoft .NET development tools, and Microsoft SharePoint.

2.1.43 REMOVED

2.1.44 Computer System Administrator

Keyport corporate IT consists of several server farms that exist locally, at various detachment sites, and at Commercial Cloud Service Provider (CCSP) Federal Risk and Authorization Management Program (FedRAMP) Impact Level Four/Five (IL4/5) environments. Server support requires specialized skills and experience in the operation of large geographically dispersed IT

infrastructures. These infrastructures may be network connected or isolated as a stand-alone enclave. Server support will consist of providing analytical and technical on-site support for the operations of Windows/Linux based servers and storage.

2.1.45 IT Asset Manager

Provide IT asset management activities in accordance with applicable IC and DoD policies, instructions, and guidance. Make recommendations to improve IT asset management processes and procedures in accordance with IC and DoD policies, instructions, and guidance. Perform IT asset management activities to support the processes of inventory, IT receiving, re-use, and disposal.

2.1.46 Drafter

Provide technical drawing support for corporate IT infrastructures to include the creation and modification of network engineering drawings, accreditation package drawings, rack elevation drawings, conceptual project drawings, and as-built drawings.

2.1.47 Project Management Support

Provide project management support using Agile software and processes established by the Government. Set up and track earned value metrics (EVM) for software projects. Monitor and document project status using Agile tools and methodologies. Perform project analysis, schedule, and cost forecasting. Compile programmatic metrics, briefings, and reports. Participate in project planning. Schedule project meetings; create and distribute meeting minutes. Assist project personnel in developing project plans and supporting documents.

2.1.48 – 2.1.51 Team Leads

The contractor shall designate Team Leads who will provide day to day supervision of the work force on site. Team Lead positions include:

- Lead Network Architect
- Lead Sr. Computer Systems Administrator
- Lead Computer User Support Specialist
- Lead Web Developer.

2.2 Key Personnel

NUMBER OF KEY PERSONNEL: ONE (1)

The following are key personnel and the requisite education and skills that apply.

2.2.1 Program Manager

The contractor shall designate a Program Manager (PM) who shall possess sufficient corporate experience and authority to manage, direct, execute and control all elements of the task order. The PM shall serve as the primary technical point of contact between the contractor and the COR, and be responsible for the coordination of all contractor technical activities related to the task order. The Program Manager shall have a substantial background in the design, development, test and support of complex software, as a participating member of technical teams.

2.3 Labor Categories, Training, Education and Experience

Table 2-1 lists the labor categories and expected individual qualifications for the support to be provided under the PWS paragraph(s) in the first column of the table. The qualifications include the following: 1) Required qualifications which are the minimum deemed necessary to successfully perform the tasking to be assigned (experience identified for each area of support may have been acquired concurrently); and 2) Desired qualifications which are those qualifications the Government would like to see in addition to the required qualifications.

Contractor personnel shall be assigned to contract efforts in a manner that will maximize productivity and efficiency. Normally, this means utilizing the lowest category of labor that is fully capable of performing a function. The contractor must utilize these categories when estimating tasks and reporting labor expenditures.

The Bureau of Labor Statistics (BLS) data provided in Table 2-1 is provided as the minimum proposal rate allowed per labor category. It reflects the government's best approximation of the BLS-defined Standard Occupational Classification (SOC) and approximate hourly rate for each Labor Category. The data is from the BLS website: http://data.bls.gov/oes/ . The geographical type used from the website is "Metropolitan or Non-Metropolitan Area", the area is "Seattle-Tacoma-Bellevue, WA", and the

period is “May 2017” (the latest data available).

The acceptable minimum hourly rate is based on the BLS data, and an escalation rate of 9% (3% per year). The escalation rate is applied to get the rates from 2017. This is for proposal purposes only, further described in Sections L & M of the solicitation.

Table C-1: Labor Categories, Training, Education and Experience Qualifications

PWS Paragraph	Description
2.1.1	**Software (Computer) Engineer**
	Required: A Four-Year or higher Math, Engineering, Computer Science, or Computer Engineering Degree from an ABET-accredited program. A minimum of three years’ experience as a C++ Application Developer.
	Desired: A minimum of three years of development and engineering experience in one or more of the following operating systems: (1) Linux, (2) Unix, and (3) Windows. Three years of experience in one or more of the following software development languages: Assembly, C, C++, and X-Windows.
	Closest BLS SOC: 15-1133, Software Developers, Systems Software
	Pay Range: $59.52 - $65.78 (-5% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $59.52
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $65.78
	Security Clearance Required: Secret
2.1.2	**Applications Software Programmer (Journeyman) - JAVA, JEE, Java Script – Description 1**
	Required: A Four-Year or higher Computer Science or Computer Engineering Degree from an ABET-accredited program. A minimum of four years of experience as a Java Application Developer.
	Desired: A minimum of one year of experience using any or all of the following technologies: (1) Hibernate, (2) Java Server Pages (JSP), (3) Angular, (4) Java Script, (5) Cascading Style Sheets (CSS), (6) JBoss, and (7) relational databases.
	Closest BLS SOC: 15-1132, Software Developers, Applications

	Pay Range: $68.04 - $78.24: (-0% to +15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $68.04
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $78.24
	Security Clearance Required: Secret
2.1.3	**Applications Software Programmer (Journeyman) - Java, JEE, Java Script – Description 2**
	Required: A Four-Year or higher Computer Science or Computer Engineering Degree from an ABET-accredited program. A minimum of four years of experience as a Java Application Developer.
	Desired: A minimum of one year of experience using any or all of the following technologies: (1) Hibernate, (2) Java Server Pages (JSP), (3) Angular, (4) Java Script, (5) Cascading Style Sheets (CSS), (6) JBoss, (7) Message Queuing, or (8) relational databases.
	Closest BLS SOC: 15-1132, Software Developers, Applications
	Pay Range: $68.04 - $78.24: (-0% to +15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $68.04
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $78.24
	Security Clearance Required: Secret
2.1.4	**Applications Software Programmer (Entry Level) - Java, JEE, Java Script**
	Required: A Four-Year or higher Computer Science or Computer Engineering Degree from an ABET-accredited program. Educational classroom experience with Java.
	Desired: Experience using any or all of the following technologies: (1) JEE, or (2) Java Script.
	Closest BLS SOC: 15-1131, Computer Programmers
	Pay Range: $49.73 - $58.01: (-10% to +5% of Annual 25th Percentile Wage)

	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $49.73
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $58.01
	Security Clearance Required: Secret
2.1.5	**Applications Software Programmer – C#, SQL, ASP .Net**
	Required: A Four-Year or higher Computer Science or Computer Engineering Degree from an ABET-accredited program or 15 years of experience in general programming. A minimum of three years of experience building and maintaining web applications using the following programming languages: C#, SQL, ASP .Net, and Java Script.
	Closest BLS SOC: 15-1132, Software Developers, Applications
	Pay Range: $61.24 - $71.44: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $61.24
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $71.44
	Security Clearance Required: Secret
2.1.6	**Applications Software Programmer – VB.Net, SQL, ASP .Net**
	Required: A Four-Year or higher Computer Science or Computer Engineering Degree or 5 years of experience in general programming.
	Desired: A minimum of three years of experience building and maintaining web applications using the following programming languages: VB.Net, SQL, ASP .Net, HTML, CSS, and Java Script.
	Closest BLS SOC: 15-1132, Software Developers, Applications
	Pay Range: $61.24 - $71.44: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $61.24
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $71.44

	Security Clearance Required: Secret
2.1.7	**Applications Software Programmer – General – Description 1**
	Required: Four years of experience as a Java Application Developer.
	Desired: A minimum of one year of experience using any or all of the following technologies: (1) Hibernate, (2) JSP, (3) Angular, (4) Java Script, (5) CSS, (6) JBoss, and (7) relational databases.
	Closest BLS SOC: 15-1131, Computer Programmers
	Pay Range: $52.49 - $58.01: (-5% to +5% of Annual 25th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $52.49
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $58.01
	Security Clearance Required: Secret
2.1.8	**Applications Software Programmer – General – Description 2**
	Required: A minimum of three years of experience building and maintaining web applications using the following programming languages: C#, SQL, .Net Core, and Java Script.
	Closest BLS SOC: 15-1131, Computer Programmers
	Pay Range: $52.49 - $58.01: (-5% to +5% of Annual 25th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $52.49
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $58.01
	Security Clearance Required: Secret
2.1.9	**Applications Software Programmer (Journeyman) – C#, SQL, .Net Core**
	Required: A Four-Year or higher Computer Science or Computer Engineering Degree from an ABET accredited school or 4 years of experience in general programming. A minimum of three years of experience building and maintaining web applications using the following programming languages: C#, SQL, .Net Core, and Java Script.

	Desired: A minimum of one year of experience using any of all of the following technologies: (1) Bootstrap, (2) JQuery
	Closest BLS SOC: 15-1131, Computer Programmers
	Pay Range: $52.49 - $58.01: (-5% to +5% of Annual 25th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $52.49
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $58.01
	Security Clearance Required: Secret
2.1.10	**Automated Test Software Programmer**
	Required: A Four-Year or higher Computer Science Degree from an ABET-accredited program. A minimum of three years of experience developing testing scripts for automated web software testing using open source automated testing applications. A minimum of two years of experience using each of the following technologies: (1) JAVA and (2) JavaScript.
	Desired: A minimum of one year of experience transitioning existing test cases into automated testing scripts.
	Closest BLS SOC: 15-1132, Software Developers, Applications
	Pay Range: $61.24 - $71.44: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $61.24
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $71.44
	Security Clearance Required: Secret
2.1.11	**Test System Software Programmer**
	Required: A Four-Year or higher Computer Science, Computer Engineering, Electrical Engineering or Electrical Engineering Technology degree from an ABET-accredited program. A minimum of three years of experience developing software for automated test equipment. A minimum three years of experience in one the following programming languages is required: (1) C#, (2) .Net Core, (3) SQL, or (4) JavaScript.

	Desired: A minimum of one year or more of experience in any or all of the following programming languages: (1) C#, (2) .Net Core, (3) SQL, or (4) JavaScript.
	Closest BLS SOC: 15-1132, Software Developers, Applications
	Pay Range: $61.24 - $71.44: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $61.24
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $71.44
	Security Clearance Required: Secret
2.1.12	**Business Analyst**
	Required: A minimum of three years of experience analyzing, compiling and documenting requirements for new or modified software application functionality.
	Desired: A Four-Year or higher Computer Science or Management of Information Systems degree from an ABET-accredited program. A minimum of three years of experience in any or all of the following areas: (1) representing user needs to the technical development team (programmers and engineers), (2) creating Use Cases, (3) reviewing development and production software for correct functionality, and (4) documenting issues and desired changes in technical detail sufficient for programmers to create or modify application code, schema, database structures, screen layouts, or application workflow.
	Closest BLS SOC: 15-1121: Computer Systems Analysts
	Pay Range: $45.64 - $55.78: (-10% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $45.64
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $55.78
	Security Clearance Required: Secret
2.1.13	**Mixed Reality Software Engineer**
	Required: A Four-Year or higher Computer Science degree from an ABET-accredited program. A minimum of two years of experience using all of the following programming languages: (1)

	C++, (2) C#, and (3) Python. A minimum of two years of experience using Unity game engine. A minimum of two years of experience creating applications for AR and VR.
	Desired: A minimum of one year of experience with the following skills and technologies: (1) Unreal game engine, (2) computer vision, (3) processing live video, (4) Bolt, (5) UI/UX design, (6) continuous integration systems, (7) 3D models, (8) Computer Aided Design and, (9) textures, materials, shaders, animations, and sounds. (10) Software design using Unified Modeling Language, (11) Testing 3D graphics applications using AR/VR, and (12) compiling and writing software documentation.
	Closest BLS SOC: 15-1132, Software Developers, Applications
	Pay Range: $61.24 - $71.44: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $61.24
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $71.44
	Security Clearance Required: Secret
2.1.14	**3D Artist – Virtual Reality**
	Required: A minimum of two years of experience in all of the following skills: (1) game design, (2) creating 3D models and sounds for virtual reality, (3) virtual reality development (4) setting up materials and shaders, and (5) creating immersive lighting and environmental effects, (6) organic modeling, (7) hard-surface modeling, (8) creation of high-level animations, (9) 3D Studio Max, (10) Maya, (11) Blender, (12) Photoshop, and (13) Substance Painter.
	Desired: A minimum of one year of experience in any or all of the following areas: (1) front-end design, (2) graphical user interface design, (4) Zbrush, (5) physically based rendering, (6) Bolt, and (7) Rigging.
	Closest BLS SOC: 15-1132, Software Developers, Applications
	Pay Range: $61.24 - $71.44: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $61.24

	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $71.44
	Security Clearance Required: Secret
2.1.15	**Software Test Engineer – Description 1**
	Required: Four-Year or higher Computer Science from an ABET-accredited program. A minimum of three years of experience developing test cases and test procedures for requirements compliance.
	Desired: A minimum of four years of experience developing test cases and test procedures for requirements compliance.
	Closest BLS SOC: 15-1132, Software Developers, Applications
	Pay Range: $61.24 - $71.44: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $61.24
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $71.44
	Security Clearance Required: Secret
2.1.16	**Software Test Engineer – Description 2**
	Required: Four-Year or higher Computer Science or Engineering Degree from an ABET-accredited program.
	Desired: A minimum of three years of experience developing test cases and test procedures for requirements compliance.
	Closest BLS SOC: 15-1132, Software Developers, Applications
	Pay Range: $61.24 - $71.44: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $61.24
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $71.44
	Security Clearance Required: Secret
2.1.17	**Software Tester – Description 1**
	Required: A minimum of one year of experience in Software Testing.
	Desired: A minimum of two years of experience in Software Testing.

	Closest BLS SOC: 15-1121: Computer Systems Analysts
	Pay Range: $45.64 - $55.78: (-10% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $45.64
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $55.78
	Security Clearance Required: Secret
2.1.18	**Software Tester – Description 2**
	Required: A minimum of one year of experience in Software Testing.
	Closest BLS SOC: 15-1121: Computer Systems Analysts
	Pay Range: $45.64 - $55.78: (-10% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $45.64
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $55.78
	Security Clearance Required: Secret
2.1.19	**General Database Administrator – Description 1**
	Required: A Four-Year or higher Computer Science or Computer Engineering Degree required. A minimum of five years of dedicated database administration experience can substitute for the education requirement. Experience with database standards and industry methodologies. Awarded and current certification(s) sufficient to be designated an Information Assurance Technician (IAT) Level II or higher in accordance with DoD 8570 requirements.
	Desired: A minimum of three years of experience in database systems and database administration including design and development.
	Closest BLS SOC: 15-1141, Database Administrators
	Pay Range: $52.27 – $60.52: (-5% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $52.27

	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $60.52
	Security Clearance Required: T5 investigation is required.
2.1.20	**General Database Administrator – Description 2**
	Required: Awarded and current certification(s) in accordance with DoD Cybersecurity Workforce policy requirements. A Four-Year or higher Computer Science or Computer Engineering Degree from an ABET-accredited program. A minimum of five years of dedicated database administration experience in combination with a professional database certification can substitute for the education requirement. A minimum of three years of experience in all of the following areas: (1) database systems and database administration including design and development. (2) database standards and industry methodologies.
	Closest BLS SOC: 15-1141, Database Administrators
	Pay Range: $52.27 – $60.52: (-5% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $52.27
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $60.52
	Security Clearance Required: T5 investigation is required.
2.1.21	**ORACLE Database Administrator**
	Required: Awarded and current certification(s) in accordance with DoD Cybersecurity Workforce policy requirements. A Four-Year or higher Computer Science or Computer Engineering Degree from an ABET-accredited program. A minimum of five years of dedicated ORACLE database administration experience in combination with ORACLE Certified Professional (OCP) certification can substitute for the education requirement. A minimum of three years of experience performing database administration of ORACLE 12c (or higher) in a Real Application Cluster (RAC) environment.
	Desired: A professional certification in any or all of the following (listed in ascending order of importance): (1) ORACLE

	Certified Associate (OCA), (2) ORACLE Certified Professional (OCP), or (3) ORACLE Certified Master (OCM). A minimum of one year of experience with any or all of the following technologies: (1) Oracle Cloud Control, (2) Recovery Manager (RMAN), and (3) web application server.
	Closest BLS SOC: 15-1141, Database Administrators
	Pay Range: $62.14 - $71.95: (-5% to +10% of Annual 75th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $62.14
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $71.95
	Security Clearance Required: T5 investigation is required.
2.1.22	**System Administrator – Description 1**
	Required: Awarded and current certification(s) in accordance with DoD Cybersecurity Workforce policy requirements. A minimum of three years of experience performing system administration of Microsoft Windows Server environment.
	Desired: Microsoft Software Engineering Certification and a minimum of one year of experience in any or all of the following: (1) Red Hat Enterprise Linux (RHEL), (2) web application server, and (3) network engineering.
	Closest BLS SOC: 15-1142, Network and Computer Systems Administrators
	Pay Range: $47.19 – $54.64: (-5% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $47.19
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $54.64
	Security Clearance Required: T5 investigation is required.
2.1.23	**System Administrator – Description 2**
	Required: Awarded and current certification(s) in accordance with DoD Cybersecurity Workforce policy requirements. A minimum of three years of experience performing system administration of Microsoft Windows

	Server and Linux/Unix environments.
	Desired: Microsoft Certified Technology Specialist (MCTS)Windows Server 2008 (or later) Network Infrastructure Configuration, Security+ Certifications, and designation of an Information Assurance Technician (IAT) Level II or higher in accordance with DoD 8570 requirements.
	Closest BLS SOC: 15-1142, Network and Computer Systems Administrators
	Pay Range: $47.19 – $54.64: (-5% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $47.19
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $54.64
	Security Clearance Required: T5 investigation is required.
2.1.24	**System Administrator – Description 3**
	Required: A minimum of three years of experience performing system administration on RedHat Enterprise Linux environments. Requires (1.) Certified Information System Security Professional (CISSP) and (2.) Security+ Certifications and designation of an Information Assurance Technician (IAT) Level II or higher in accordance with DoD 8570 requirements.
	Desired: Any or all of the following certifications: (1) RedHat Certified Engineer (RHCE), (2) RedHat Certified Systems Administrator (RHCSA), (3) Network+, or (4) Cisco Certified Network Associate (CCNA)
	Closest BLS SOC: 15-1142, Network and Computer Systems Administrators
	Pay Range: $47.19 – $54.64: (-5% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $47.19
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $54.64
	Security Clearance Required: T5 investigation is required.

2.1.25	**User Interface Designer**
	Required: A two-year Graphics Design or Web Design degree with a User Experience (UX) Design emphasis. A minimum of three years of experience designing User Interfaces (UI) for web based applications.
	Desired: A minimum of two years of experience in any or all of the following: (1) working with customers to develop and document UI requirements and design sufficient for software developers to create or modify screen layouts and (2) two years' experience using UI modeling tools.
	Closest BLS SOC: 15-1134, Web Developers
	Pay Range: $60.19 – $66.53: (-5% to +5% of Annual 75th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $60.19
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $66.53
	Security Clearance Required: Secret
2.1.26	**Application Support Specialist**
	Required: A minimum of two years of experience both providing middle tier (Level 2) application support and supporting relational database systems using SQL.
	Desired: One year of experience using PL/SQL
	Closest BLS SOC: 15-1151, Computer User Support Specialists
	Pay Range: $30.20 – $33.22: (-0% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $30.20
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $33.22
	Security Clearance Required: Secret
2.1.27	**IT Technical Writer**
	Required: A minimum of two years of experience in Technical Writing.
	Closest BLS SOC: 27-3042, Technical Writers

	Pay Range: $40.41 – $44.66: (-5% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $40.41
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $44.66
	Security Clearance Required: Secret
2.1.28	**Cyber Security Support Analyst – Description 1**
	Required: Awarded and current certification(s) in accordance with DoD Cybersecurity Workforce policy requirements. A minimum of two years of experience in each of the following tasks: (1) preparing system accreditation documentation required by the Navy and/or DoD, (2) evaluating security configurations of systems, and (3) maintaining security configurations of production, development and test systems by applying and configuring security controls.
	Desired: A minimum of one year of experience with any or all of the following DoD Cybersecurity assessment and compliance tools: (1) eMASS, (2) Assured Compliance Assessment Solution (ACAS) and (3)Host Based Security System (HBSS).
	Closest BLS SOC: 15-1122, Information Security Analysts
	Pay Range: $51.95 - $60.61: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $51.95
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $60.61
	Security Clearance Required: T5 investigation is required.
2.1.29	**Cyber Security Support Analyst – Description 2**
	Required: A minimum of two years of experience in each of the following tasks: (1) preparing system accreditation documentation required by the Navy and/or DoD, (2) Assessing system vulnerability using approved DOD tools. Awarded and current certification(s) sufficient to be designated as Cyber Security Workforce Risk Management -

	Advanced or Information System Security Management -Advanced (CSWF Specialty Areas 61 or 72 respectively) in accordance with DoD 8140.01.
	Desired: A minimum of one year of experience in each of the following tasks: (1) evaluating security configurations of systems, and (2) maintaining security configurations of production, development and test systems by applying and configuring security controls.
	Closest BLS SOC: 15-1122, Information Security Analysts
	Pay Range: $51.95 - $60.61: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $51.95
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $60.61
	Security Clearance Required: T5 investigation is required.
2.1.30	**Cyber Security Support Analyst – Description 3**
	Required: Awarded and current certification(s) in accordance with DoD Cybersecurity Workforce policy requirements. A minimum of two years of experience in each of the following tasks: (1) preparing system accreditation documentation required by the Navy and/or DoD, (2) evaluating security configurations of systems, and (3) maintaining security configurations of production, development and test systems by applying and configuring security controls.
	Desired: A minimum of one year of experience with any or all of the following DoD Cybersecurity assessment and compliance tools: (1) eMASS, (2) Assured Compliance Assessment Solution (ACAS) and (3) Host Based Security System (HBSS).
	Closest BLS SOC: 15-1122, Information Security Analysts
	Pay Range: $51.95 - $60.61: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $51.95

	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $60.61
	Security Clearance Required: T5 investigation is required.
2.1.31	**Cyber Security Support Analyst – Description 4**
	Required: A minimum of two years of experience in each of the four following tasks: (1) preparing system accreditation documentation required by the Navy and/or DoD, (2) evaluating security configurations of systems, and (3) maintaining security configurations of production, development and test systems by applying and configuring security controls, and (4) assessing system vulnerability using approved DOD tools. Awarded and current certification(s) sufficient to be designated as Cyber Security Workforce Risk Management - Advanced or Information System Security Management -Advanced (CSWF Specialty Areas 61 or 72 respectively) in accordance with DoD 8140.01.
	Closest BLS SOC: 15-1122, Information Security Analysts
	Pay Range: $51.95 - $60.61: (-10% to +5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $51.95
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $60.61
	Security Clearance Required: T5 investigation is required.
2.1.32	**Cyber Operations Engineer**
	Required: A minimum of four years of experience performing advanced information operations/cyber security functions that include advanced vulnerability assessment(s) and cyber threat analysis of systems and applications with or without automated tools. Ability to analyze developed and procured software code for security vulnerabilities and/or conduct penetration testing of software with or without automated tools. Awarded and current certification(s) sufficient to be designated an Information Assurance Technician (IAT) Level II or higher in accordance with DoD 8570 requirements.

	Closest BLS SOC: 15-1133, Software Developers, Systems Software
	Pay Range: $59.52 - $68.92 (-5% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $59.52
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $68.92
	Security Clearance Required: T5 investigation is required.
2.1.33	**Network Technician**
	Required: A minimum of three years of experience performing network cable plant operations including cable terminations, cable routing, network rack configuration, and switch configurations.
	CompTIA Security + and/or International Information Systems Security Certification; Consortium ((ISC)2) Systems Security Certified Practitioner (SSCP); Certified Network Associate certification and/or Current Cisco Certified Network Associate-Voice Certification; Fiber Optic cable installation and termination (Certified Fiber Optics Installer (CFOI) certification).
	Closest BLS SOC: 15-1152, Computer Network Support Specialist
	Pay Range: $38.76 - $44.57 (+0% to +15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $38.76
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $44.57
	Security Clearance Required: T5 investigation is required.
2.1.34	**Corporate VoIP Operation and Support**
	Required: A minimum of three years of experience performing enterprise Voice over Internet Protocol operations and maintenance and the Cisco Unified Communications platform including Call Manager, Unity, and Cisco Emergency Responder.
	CompTIA Security + and/or International Information Systems Security Certification; Consortium ((ISC)2) Systems Security Certified Practitioner (SSCP); Certified Network Associate

	certification and/or Current Cisco Certified Network Associate-Voice Certification; Fiber Optic cable installation and termination (CFOI certification).
	Closest BLS SOC: 15-1142, Network and Computer Systems Administrators
	Pay Range: $47.19 – $54.64: (-5% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $47.19
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $54.64
	Security Clearance Required: T5 investigation is required.
2.1.35	**Computer User Support Specialist 1**
	Required: A minimum of four years of experience in the management and resolution of Tier 2 levels IT Support Services tickets. Thorough knowledge in the configuration, deployment and troubleshooting Microsoft desktop Operating Systems, desktop productivity applications, desktop defense tools, Microsoft Active Directory account management and permissions, basic network connectivity troubleshooting.
	CompTIA Security + and/or ISC2 SSCP, Current Microsoft Desktop and Server OS Certification
	Desired: ITIL Foundation Certification
	Closest BLS SOC: 15-1151, Computer User Support Specialist
	Pay Range: $38.64 - $42.51 (+0% to +10% of Annual 75th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $38.64
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $42.51
	Security Clearance Required: T5 investigation is required.
2.1.36	**Computer User Support Specialist 2**
	Required: A minimum of two years of experience in the management and resolution of Tier 2 levels IT Support Services tickets. Practical knowledge in the configuration, deployment and troubleshooting Microsoft desktop

	Operating Systems, desktop productivity applications, desktop defense tools, Microsoft Active Directory account management and permissions, basic network connectivity troubleshooting.
	CompTIA Security + and/or ISC2 SSCP, Current Microsoft Desktop OS Certification
	Desired: ITIL Foundation Certification
	Closest BLS SOC: 15-1151, Computer User Support Specialist
	Pay Range: $30.20 - $34.74 (+0% to 15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $30.20
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $34.74
	Security Clearance Required: T5 investigation is required.
2.1.37	**Video Teleconference (VTC) Support Specialist**
	Required: A minimum of three years of experience with H.323 and H.320 video conferencing technologies to include setup and tear-down of calls and bridging disparate VTC systems Ability to perform VTC troubleshooting and diagnostics.
	CompTIA Security + and/or ISC2 SSCP
	Desired: Three (3) years of experience with collaborative technologies and integration with VTC technologies.
	Closest BLS SOC: 15-1151, Computer User Support Specialist
	Pay Range: $30.20 - $34.74 (+0% to 15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $30.20
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $34.74
	Security Clearance Required: T5 investigation is required.
2.1.38	**Hardware/Software Management Support**
	Required: A minimum of three years with DoD IT procurement experience.

	Desired: A minimum of three years of experience or more with DoD, IT procurements, Knowledge of the DoN ITPR process and DON Application and DADMS.
	Closest BLS SOC: 43-9011, Computer Operators
	Pay Range: $26.57 - $30.56 (+0% to 15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $26.57
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $30.56
	Security Clearance Required: Secret
2.1.39	**Telecommunications Support**
	Required: A minimum of three years of full-time professional experience working with voice and data circuits and professional experience working with the DISA Direct Order Entry (DDOE) process.
	Closest BLS SOC: 49-2022, Telecommunications Equipment Installers and Repairers, Except Line Installers
	Pay Range: $32.94 - $38.14 (-5% to +15% of Annual 75th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $32.94
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $38.14
	Security Clearance Required: Secret
2.1.40	**IT Configuration Manager**
	Required: A minimum of five years of full-time experience developing and managing an ITIL/ITSM based Configuration Management (CM) program.
	Desired: ITIL or ITSM Foundation Certification
	Closest BLS SOC: 15-1121, Computer Systems Analysts
	Pay Range: $37.78 - $44.08 (-10% to +5% of Annual 25th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $37.78

	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $44.08
	Security Clearance Required: Secret
2.1.41	**Web Developer 1**
	Required: A minimum of five years of experience designing, building, and maintaining web sites using commercial framework tools.
	Closest BLS SOC: 15-1134, Web Developers
	Pay Range: $48.89 – $56.22: (+0% to +15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $48.89
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $56.22
	Security Clearance Required: T5 investigation is required.
2.1.42	**Web Developer 2**
	Required: A minimum of three years of experience designing, building, and maintaining web sites using commercial framework tools.
	Closest BLS SOC: 15-1134, Web Developers
	Pay Range: $34.64 – $38.28: (-5% to +5% of Annual 25th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $34.64
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $38.28
	Security Clearance Required: T5 investigation is required.
2.1.43	**REMOVED**
2.1.44	**System Administrator**
	Required: A minimum of two years of full-time professional experience working with the configuration, deployment, and operation and maintenance of Microsoft and Linux server operating systems. A minimum two (2) years specific experience in managing Microsoft Active Directory, Domain Name Service (DNS) and DHCP services. CompTIA Security + and/or ISC2 SSCP, Current Microsoft Server

	and/or VMware VCP Certification
	Desired: A minimum of two (2) years' experience in the operation of Storage Area Networking (SAN) and storage systems, and at least two (2) years' experience in the operation of VMware Virtualization technologies and understanding of Microsoft SQL server and clustering technologies.
	Closest BLS SOC: 15-1142, Network and Computer Systems Administrators
	Pay Range: $47.19 – $54.64: (-5% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $47.19
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $54.64
	Security Clearance Required: T5 investigation is required.
2.1.45	**IT Asset Manager**
	Required: A minimum of three years of experience in asset management support providing inventory, storing, tracking and disposition support. A minimum of two (2) years or more years of experience in the management and resolution of IT Support Services tickets.
	Desired: ITIL Foundation Certification, CompTIA Security + and/or ISC2 SSCP, Current Microsoft Desktop OS Certification
	Closest BLS SOC: 15-1151, Computer User Support Specialist
	Pay Range: $30.20 - $34.74 (+0% to 15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $30.20
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $34.74
	Security Clearance Required: Secret
2.1.46	**Drafting Technician**

	Required: A minimum of two years of experience creating detailed technical drawings. A minimum of two (2) or more years of experience with Microsoft Visio and Computer Aided Design tools.
	Desired: Two (2) or more years of experience creating and modifying Information Technology infrastructure drawings to include network layouts, rack elevation drawings, and system concepts.
	Closest BLS SOC: 17-3019, Computer User Support Specialist
	Pay Range: $31.14 - $35.82 (+0% to +15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $31.14
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $35.82
	Security Clearance Required: Secret
2.1.47	**Project Management Support Analyst**
	Required: A minimum of three years of experience using Agile methodologies to set up and track earned value metrics for software projects. A minimum of three years of experience performing project analysis, monitoring schedules, and performing cost forecasting.
	Desired: Three years of experience in any or all of the following software applications: (1) Microsoft Excel, (2) PowerPoint, (3) Project, and (4) Word.
	Closest BLS SOC: 17-3019, Computer User Support Specialist
	Pay Range: $31.14 - $35.82 (+0% to +15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $31.14
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $35.82
	Security Clearance Required: Secret
2.1.48	**Lead Network Architect**
	Required: A minimum of: five years of professional experience in design, implementation, and operation of a geographically dispersed network including LAN/WAN coaction and circuits; three years professional experience managing and operating Cisco

	VoIP and in the securing and hardening of networking technologies. Cisco Certified Network Professional (CCNP),
	CompTIA Security + and/or ISC2 Systems Security Certified Practitioner (SSCP)
	Desired: ISC2 Systems Certified Information Systems Security Professional (CISSP).
	4-yr degree from an ABET accredited program in Information Technology or Engineering discipline.
	Closest BLS SOC: 15-1143, Computer Network Architect
	Pay Range: $55.50 - $64.27 (-5% to +10% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $55.50
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $64.27
	Security Clearance Required: T5 investigation is required.
2.1.49	**Lead Senior Computer Systems Administrator**
	Required: A minimum of five years of full-time professional experience working with the configuration, deployment, and operation and maintenance of Microsoft and Linux server operating systems. A minimum five (5) years specific experience in managing Microsoft Active Directory, DNS and DHCP services. A minimum of five (5) years' experience in the operation of Storage Area Networking (SAN) and storage systems, and at least three (3) years' experience in the operation of VMware Virtualization technologies and understanding of Microsoft SQL server and clustering technologies. CompTIA Security + and/or ISC2 SSCP, Current Microsoft Server and/or VMware VCP Certification
	Desired: Certification in Storage Area Networking technology such as NetApp or SNIA Certified Storage Professional (SCSP).
	Closest BLS SOC: 15-1142, Network and Computer Systems Administrators
	Pay Range: $47.19 – $54.64 : (-5% to +10% of Annual Median Wage)

	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $47.19
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $54.64
	Security Clearance Required: T5 investigation is required.
2.1.50	**Lead Computer User Support Specialist**
	Required: A minimum of five years of experience in leading a Tier 2 IT Support Service operations including the management, prioritization, scheduling, and resolution of IT Support Service tickets. A minimum of five years of full-time professional experience working with the configuration, deployment, and operation and maintenance of Microsoft and Linux desktop operating systems.
	CompTIA Security + and/or ISC2 SSCP, Current Microsoft Desktop and Server OS Certification.
	Desired: ITIL Foundation Certification
	Closest BLS SOC: 15-1151, Computer User Support Specialist
	Pay Range: $38.64 - $42.51 (+0% to +10% of Annual 75th Percentile Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $38.64
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $42.51
	Security Clearance Required: T5 investigation is required.
2.1.51	**Lead Web Developer**
	Required: A minimum of five years of analyzing user requirements; envisioning system features and functionality; designing and developing user interfaces; determining design methodologies; completing programing using visual studio, NET, Java, C#; designing and conducting testing.
	CompTIA Security + and/or ISC2 SSCP
	Desired: 4-yr degree from an ABET accredited university from accredited college in Computer Science or Computer Engineering Degree.
	Closest BLS SOC: 15-1134, Web Developers

	Pay Range: $48.89 – $56.22: (+0% to +15% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $48.89
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $56.22
	Security Clearance Required: T5 investigation is required.
Key Personnel	
2.2.1	**Program Manager**
	Required: A minimum of five years of experience in building and managing software development teams using technologies and skill categories listed in paragraphs 2.1 to 2.4.
	Desired: Desired: ISC2 Systems Certified Information Systems Security Professional (CISSP) and/or Project Management Professional (PMP)
	Closest BLS SOC: 11-3021, Computer and Information System Manager
	Pay Range: $74.02 - $81.81 (-5% to + 5% of Annual Median Wage)
	Minimum Hourly Rate in Proposal for Base Year (Option Years must be escalated): $74.02
	Evaluated Hourly Rate for Base Year (Option Years will be escalated) if Offeror did not Propose the Minimum or Greater: $81.81
	Security Clearance Required: Secret

3.0 GENERAL INFORMATION/REQUIREMENTS

3.1 Hours of operation

Normal hours of operation at NUWC Keyport are from 0700-1530 Pacific Time, Monday through Friday, except Federal holidays. Alternate work schedules must be approved by the COR, and must not negatively impact task order deliverables or project schedules. Teleworking may be permitted on a situational basis. Approval to telework must be approved by the COR. Upon completion of teleworking, the contractor must submit a telework report to the Program Manager detailing the work accomplished during the telework hours by close of business the following work day.

NUWC Keyport is normally closed between 25 December and 1 January each year. Contractor personnel performing on-site services at Keyport will not work on-site at Keyport during this time frame without Contracting Officer approval.

3.2 Overtime

Overtime is anticipated at a total of 17,900 hours for the base year and all option years (4,475 hours per year) and is included in the total hours provided in Attachment 03 Estimated Level of Effort. Overtime shall be coordinated with the COR with an approved Technical Instruction Letter, prior to use. Overtime that is not approved in advance shall not be authorized for payment. Should the need arise in such a manner that written authorization is not possible, a verbal authorization shall be obtained from the Contracting Officer to be followed up in writing within three (3) working days.

3.3 Government Facilities/Office Space

Services require the contractor to work within NUWC Keyport. The government will provide access to computer resources, information systems and databases, software versioning and version control systems for the check-out and check-in of developed and modified code, and software defect tracking applications and databases. Additionally, the Government will provide the contractor access to all related programs, technical data, training materials, life-cycle support equipment, and information located at NUWC Keyport that is necessary to provide the specified services. The Government will provide work space, telephone, computer, and office supplies as well as access to the classified and unclassified systems and servers for software being developed under this task order. The contractor is responsible for providing transportation services to and from the work site. While working at Government facilities the contractor shall follow all local regulations and guidance for workplace safety. The contractor shall adhere to industry safety standards and local guidance on cleanliness of the work area.

3.4 Management Plan

The contractor shall develop and submit to the government a Management Plan (CDRL A001). The plan shall establish and maintain a management program to be used during task order performance, incorporating details of the requirements set forth in this PWS. The management plan must reflect an understanding of all tasks and performance objectives specified in this PWS and describe an approach to satisfy these requirements. At a minimum, the plan shall identify all contractor resources; i.e., equipment, material, supplies, and staffing plan detailing how these resources will enable the contractor to meet performance objectives. Distribution Code D (DoD and DoD Contractors Only) applies to the Management Plan.

3.4.1 Quality Control

In Section 3.2e of the contractor’s Management Plan, the contractor shall describe their Quality Control Program. The Contractor is solely responsible for the quality of services provided. The Contractor is also liable for Contractor employee negligence, and any fraud, waste or abuse. As part of Program Management, the Contractor shall utilize a Quality Control Program to ensure that services are completed in accordance with acceptable principles of internal control, and meet specified, acceptable levels of quality. There shall be a method to identify deficiencies in services that may occur and procedures to correct any deficiency in services that may occur. Execution of the Quality Control Program shall be documented and made available to the Government during the period of performance.

3.4.2 Quality Assurance

The Government will monitor the Contractor's performance. The Government reserves the right to review services to be provided, including those developed or performed at the Contractor's facilities, to determine conformance with performance and technical requirements. Government quality assurance will be conducted on behalf of the Contracting Officer. The COR will be appointed to coordinate the overall quality assurance of technical compliance. The contractor shall develop quality control procedures that address the areas identified in the Acceptable Quality Levels (AQLs) identified in Attachment 04, Performance Requirements Summary.

3.4.3 Subcontractor Management

The contractor is responsible for performance requirements delineated in this PWS, and shall institute appropriate management actions relative to subcontractor performance. Requirements that are contractually specified shall apply to subcontractor performance; however, the contractor shall be accountable for compliance of subcontractors and is responsible for ensuring all deliverable products comply with task order requirements.

3.5 Environmental Compliance Requirements

The Contractor shall comply, and ensure that all subcontractors comply, with all applicable environmental federal, state, and local laws and regulations and Navy policies, instructions, plans, and ISO 14001 Environmental Management System. The contractor shall comply with all federal, state, local and Navy environmental compliance training requirements. The contractor shall comply with all environmental regulatory agency permit conditions and consultation requirements. The contractor shall be liable for all of their Notice of Violations (NOV), fines, penalties, and corrective actions imposed by federal, state or local environmental regulatory agencies due to the contractor's inability to comply with environmental requirements. These costs will not be reimbursed. The contractor shall provide verbal notification to the COR and the Government Technical Representative (GTR) within 24 hours of receiving a NOV or equivalent followed by written notification within three (3) workdays of receiving a NOV.

Hazardous Waste and Material Control/Handling: The contractor shall comply with all Navy instructions applicable, e.g., but not limited to OPNAV M-5090.1D Environmental Readiness Program Manual, NUWCDIVKPT 5090K, Environmental Program Policy and Manual, and KPT 5090-09K Hazardous Waste Management Program. The NAVSEA NUWC Division Keyport "Contractors Guide to Environmental Policy" is hereby incorporated in full by reference. The guide offers the level of detail needed to comply with key environmental regulations, and is designed to meet the environmental information needs of contractors working at the facility.

3.6 Safety

The contractor shall comply with the latest applicable federal and state laws, regulations and management plans and requirements regarding occupational safety and health. In the event that safety laws, regulations or requirements change during the term of the contract, the contractor is required to comply as such laws come into effect. While working on government facilities the contractor shall follow all local regulations and guidance for workplace safety including electronics, explosives, crane, and Electrostatic Discharge (ESD) requirements. The contractor shall adhere to industry safety standards, material safety data sheets (MSDS) for handling hazardous material and local guidance on cleanliness of the work area.

Work to be performed under this contract must be accomplished in accordance with safety and health standards and directives pursuant to the Occupational Safety and Health Act of 1970, Public Law 91-596. Numerous safety and health standards exist that apply to operations at NUWC Division KPT. These include but are not limited to 29 CFR 1910 General Industry Standards, 29 CFR 1915 Maritime Standards, 29 CFR 1926 Construction Standards, WAC-296-24-14529 General Safety and Health Standards (Washington State), EM385-1-1 Safety and Health Requirements Manual (U.S. Army Corps of Engineers), Unified Facilities Guide Specifications UFGS-01 35 26 (April 2008), and the NAVSEA NUWC Division Keyport Safety Requirements for Contractors and Subcontractors.

3.7 Performance Requirements Summary

The PRS table provided as Attachment 04 to Section J identifies the mission critical items for performance under this contract. Only performance deficiencies that are directly attributable to contractor error are considered when measured against the performance threshold.

3.8 Technical Instructions

Based on the requirements contained in the PWS, the contractor shall be issued TI Letter by the COR. The contractor shall ONLY accept officially approved TI's. All approved TI's will be signed, dated by the COR and the Contracting Officer, and provided by the COR for Contractor Signature. The TI may be signed electronically. No work shall begin before the TI is finalized.

3.9 Security Requirements

3.9.1 Security Classification of Equipment, Components, Spaces and Documents

The Equipment, Components, Spaces or Documents used may be classified and are subject to the applicable provisions of DoD 5220.22M, National Industrial Security Program Manual; SECNAV M-5510.36, DON Information Security Program Manual; SECNAV M- 5510.30, Personnel Security Program Manual; NUWCDIVKPT 5510, Information and Personnel Security Programs; NUWCDIVKPT 5530.1, Physical Security Manual; and the NUWC Information Assurance Program Manual, NUWCDIVKPT 5239.1E.

Contractor personnel supporting this task order who require access to classified Spaces, Equipment, or Documents will require a security clearance equivalent to the level of access required to complete assigned duties.

Security Education: Per SECNAV M-5510.36 (11-4.2.a), contractor employees embedded in government work spaces shall be included in the command security education program (i.e. review each Security Training Quarterly Bulletin & those with Secret or above security clearances must attend a locally provided NCIS counterintelligence briefing annually).

3.9.2 Privacy Act, Classified and Proprietary Data Handling

Work done under this contract involves data subject to the Privacy Act of 1974 (5 U.S.C. 552a) and must be safeguarded in accordance with that Act. When Privacy Act data is passed to the contractor to be used on non-Navy systems and networks —either electronically or in hard copy—the contractor will be required to sign for receipt. If Privacy Act, classified or proprietar data is compromised or lost the contractor must immediately inform the contracting officer or the COR and report the surrounding

details. Work done under this contract involves proprietary data that requires contractor personnel to sign Non-Disclosure agreements.

3.9.3 Contractor Personnel

Contractor personnel supporting this Task Order require a security clearance level of up to Top Secret as noted in Table 2-1; but with no lower than the level of access required to complete the assigned duties. For contractor employees carrying out work under this PWS, access to Government facilities and networks will be through Common Access Card (CAC) credentials controlled by the Trusted Associate Sponsorship System (TASS). Both physical access and logical access is required to be eligible for a CAC.

Please note the following:

- TASS requires Background Vetting for applicants, including a valid National Agency Check with Inquires (NACI) and an FBI fingerprint check with favorable results.

-Within 30 days of task order award, the Contractor shall identify those personnel requiring and eligible for CACs. The COR acting as Trusted Agent (TA) under TASS will initiate CAC applications in TASS based on data received from the contractor. The Contractor shall minimize delays resulting from CAC requirements through effective management of changes to the workforce.

3.9.4 Privileged Access

In accordance with Secretary of Navy Instruction (SECNAVINST) SECNAVINST 5510.30 Paragraph 5-3, subparagraphs b (6) (a), b (6) (e), b (6) (f), b (6) (g), and Exhibit 5A, Performance requirements are at the IT-1 Critical Sensitive position for contractors performing these functions. The IT-1 positions require full positive adjudication of a Single Scope Background investigation. Additionally, per DOD Manual 8570-1M (Change 3): C2.3.8 Contractor personnel supporting IA functions shall obtain the appropriate DOD-approved IA baseline certification PRIOR to being engaged. Additional training on local or system operating systems or procedures must be met within 6 months of engagement. C3.2.3.3 Contract personnel must comply with the DOD and Vendor CEU requirements to maintain their IA baseline certification. Tables C3.T4, C3.T5, Paragraphs C7.3.4 and AP3.1.5, performance requirements will be set at the Information Assurance Technical (IAT) level II and all training and certification specification are required to be met for any contracted employee. Secretary of Navy Manual (SECNAVMAN) SECNAVMAN 5239.2 IA Workforce Management Manual provides additional amplifying policy and requirements.

The following contractor personnel from Table 2-1 will have Privileged Access and be designated as part of the Information Assurance Workforce in accordance with DoD 8570:

- General Database Administrator (paragraph 2.1.19/20)

- Oracle Database Administrator (paragraph 2.1.21)

- System Administrator (paragraph 2.1.22/23/24)

- Cyber Security Support Analyst (paragraph 2.1.28/29/30/31)

- Cyber Operations Engineer (paragraph 2.1.32)

- Network Technician (paragraph 2.1.33)

- Corporate VoIP Operation and Support (paragraph 2.1.34)

- Computer User Support Specialist (paragraph 2.1.35/36)

- Video Teleconference Support Specialist (paragraph 2.1.37)

- Web Developer (paragraph 2.1.41/42)

- System Administrator (paragraph 2.1.44)

- Lead Network Architect (paragraph 2.1.48)

- Lead Computer Network Administrator (paragraph 2.1.49)

- Lead Computer User Support Specialist (paragraph 2.1.50)

- Lead Web Developer (paragraph 2.1.51)

These personnel will be required to have a favorably adjudicated SSBI before beginning work on this contract. In order to obtain the SSBI, personnel must be investigated at the Top Secret level.

3.9.5 Information Assurance Training

Contractor personnel supporting this task order who require access to DoD Information Systems are required to receive and complete initial IA orientation awareness training before being granted access to the system(s), and annual IA awareness training to retain access, as required In Accordance With (IAW) DoD 8570.01-M and Department of Defense Instruction (DoDI) 8500.2 E3.3.7. Access requests to DoD IT systems will utilize OPNAV 5239/14 (July 2008) SAAR-N form.

3.9.6 Operations Security (OPSEC) Requirements

Performance under this contract requires the contractor to adhere to OPSEC requirements. Explanation of these requirements is detailed in the Operations Security Guide for Defense Contractors, available online at:

http//www.navsea.navy.mil/Home/WarfareCenters/NUWCKeyport/Resources.aspx; click on the OPSEC guide for Defense Contractors on the left hand side.

4.0 BASIS OF ESTIMATE

Attachment 03 provides the government's estimate of the labor categories and cumulative hours required to execute the anticipated tasks in support of the Integrated Product Team efforts. In each of these efforts, government personnel will retain responsibility for the inherently governmental functions of technical direction of products, overall prioritization of work efforts, and design, functionality and system engineering decisions. Management and supervision of contractor work efforts and deliverables remain the responsibility of offeror's personnel.

The Program Management hours, such as, the management, supervisory and administrative (security, human resources, etc.) efforts of the offeror are not reflected in the government's estimate of labor categories and contract hours required that are shown in Attachment 03.

4.1 Task 1: Aircraft Carrier Tactical Support Center (CV-TSC) Support and Undersea Warfare Decision Support System (USW-DSS) Support

The AN/SQQ-34, CV-TSC system, is an aircraft carrier based Undersea Warfare (USW)/Surface Warfare (SUW) combat system designed to maintain tactical situation awareness and support command and control functions in conjunction with the Ship Self Defense System (SSDS). NUWC Keyport, as the Design Agent (DA) and In-Service Engineering Agent (ISEA) provides advanced software development capability as well as support of fleet fielded systems. CV-TSC is developed in a Distributed Object Processing Framework implemented in the Java programming language, containing approximately 50 Computer Software Configuration Items (CSCIs).

The AN/UYQ-100, USW-DSS system is a surface ship-based situation awareness and mission planning combat system for anti-submarine warfare. NUWC Keyport, as the ISEA provides direct support to the fleet, keeping the systems operational. The USW-DSS Computer Software Configuration Items (CSCIs) are supported by multiple OEMs and or government activities. The software contains approximately 19 CSCIs written in C, C++, Java, and Ruby. USW-DSS runs on RedHat Enterprise Linux 5.x.

SYSTEM ARCHITECTURE(S) / SOFTWARE TECHNOLOGIES	CURRENT DEPLOYMENT / UTILIZATION

SYSTEM ARCHITECTURES: RedHat Enterprise Linux. May include versions such as C/C++ and Distributed Object Processing Framework implemented in the Java programming language, and run on RedHat Enterprise Linux operating systems. SOFTWARE TECHNOLOGIES: C, C++, Java, JavaScript, JEE, Visual Studio, Team Foundation Server	Deployed on Aircraft Carriers, shore sites, watch floors and training sites

For the CV-TSC program, or similar programs or projects, perform the functions in paragraphs 4.1.1 - 4.1.10. The Government estimate of labor categories and cumulative hours required is in Attachment 03. For paragraphs 4.1.1 – 4.1.4 the levels of complexity for the 25 functional use cases are 5 high, 15 medium, and 5 low.

4.1.1 Software (Architect) Engineering for Capability Improvements

For estimation purposes, assume system capability increase is composed of 25 functional use cases across the architecture, user interface and external interfaces. Based on the top level requirements, software systems engineering analysis shall be performed and design artifacts created and/or updated for software architecture, design, development and test. For estimating purposes, assume one System Requirements Specification, one System Architecture and Requirements Allocation Description, one Software Architecture Description, one Software Requirement Specification, one Runtime Architecture Description and 25 Software Functional Descriptions.

4.1.2 Software Development for Capability Improvements

For estimation purposes, assume one system software capability release per year. Also assume system software capability increase is composed of 25 functional use cases and the required software capability will be described in a Software Requirement Specifications; this will include software engineering, use cases and sequence diagrams to provide sufficient technical detail for application programmers (proficient in Java, JEE and Java Script) to perform detailed design, software coding, source code review, test case development, and user documentation. The capability is to be developed in 8 software sprint rounds, each sprint round being 6 weeks. Each sprint includes the detailed design, software coding, source code review, test case development, and user documentation.

4.1.3 System Test Engineering for Capability Improvements

For estimation purposes, assume system capability increase is composed of 25 functional use cases across the architecture, user interface and external interfaces. Based on design artifacts, created through software systems engineering, system test engineering shall be performed and include development of test plans, test scenarios, test cases and test reports for system capability requirements compliance. For estimating purposes, assume 13 test plans, 25 test scenarios, 150 test cases, 13 test reports and defect reporting metrics.

4.1.4 Software Test Engineering for Capability Improvements

For estimation purposes, assume system capability increase is composed of 25 functional use cases across the architecture, user interface and external interfaces. Based on design artifacts, created through software systems engineering, software test engineering shall be performed and include development of test scenarios, test cases, test reports and defect reports for system capability requirements compliance. For estimating purposes, assume 25 test scenarios, 150 test cases, and 13 test reports.

4.1.5 Software Testing for Capability Improvements

For estimation purposes, assume ad hoc testing to support software sprints. Execute test procedures; write trouble reports (TRs) for defects and deficiencies. For estimating purposes, assume 150 test cases and 300 test procedures.

4.1.6 Software Defect Fixes and Maintenance

For estimation purposes, assume one software release per year with each comprised of 15 defect fixes. The complexities of the modifications are as follows: 5 high, 5 medium, and 5 low. Software fixes require proficient Java, JEE and Java Script application programmers to perform/update detailed design, software coding, source code review, test case development, and user

documentation. For estimating purposes, assume 2 software sprint rounds, each sprint round being 6 weeks. Each sprint includes the detailed design, software coding, source code review, test case development, and user documentation.

4.1.7 System Administration

For estimation purposes, assume annual maintenance of network integrity and connectivity, maintenance of software development workstation configurations, ensuring compliance with information security policies and maintaining system backup and recovery. Ensure compliance through use of scanning tools and provide mitigation as required. For estimating purposes, assume the development environment will have 20 software development workstations, 10 IAVA per month, and 2 STIG per month.

4.1.8 Technical Writer

For estimation purposes, assume the generation of technical documents from software engineering artifacts such as use cases, sequence diagrams and help files. For estimating purposes, assume 50 use cases, 50 sequence diagrams, and 50 help files.

4.1.9 Travel

Travel will be required in support of this effort as reflected in paragraph 4.14. All travel will be directed by the COR through TI's.

4.2 Task 2: Removed

4.2.1 System Administration

For estimation purposes, assume maintenance activities ensuring compliance with information security policies. Ensure compliance through use of scanning tools and provide mitigation as required. For estimating purposes, assume 5 IAVAs per month, and 1 STIG per month.

4.2.2 Travel

No travel required.

4.3 Task 3: Countermeasures Set Acoustic (CSA) and Tactical Decision Aid (TacDA) Support

The CSA and TacDA are based on real-time or near real-time embedded computing architecture and serve as a stand-alone Ship Self-Protect (SSP) system. Variants have been programmed in multiple languages, predominantly C and C++, for multiple computing platforms. Development operating systems include Windows and Linux; target operating systems include Linux and VxWorks. The submarine launched countermeasures ISEA team provides direct technical, software and logistics support to the fleet, ensuring the availability of the CSA and External Countermeasure Launcher launch systems and the countermeasure devices.

SYSTEM ARCHITECTURE(S) / SOFTWARE TECHNOLOGIES	CURRENT DEPLOYMENT / UTILIZATION
SYSTEM ARCHITECTURES: Embedded IDAN form factor using Red Hat Enterprise Linux, Embedded Kontron system using Red Hat Enterprise Linux, Embedded ATX form factor using Red Hat, and Embedded system using Atmel processor SOFTWARE TECHNOLOGIES: C, C++, X Display, Assembly	Deployed aboard submarines

For the Countermeasures Program, perform the functions in paragraphs 4.3.3 - 4.3.4. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.3.1 Removed

4.3.2 Removed

4.3.3 Technical Writer

For estimation purposes, assume the generation of technical documents from software engineering artifacts such as use cases, sequence diagrams and help files. For estimating purposes, assume 12 use cases, 12 sequence diagrams, and 12 help files.

4.3.4 Travel

No travel required.

4.4 Task 4: Advanced Skills Management Support

The ASM system is Navy-developed and owned and in full production. ASM is a Training Management System (TMS). It supports the defining, assigning, tracking and attaining of any type of qualification, certification or license required by workforce members. The system provides individual, unit and rollup visibility into readiness, and provides readiness reporting tools. ASM interfaces with numerous other training and qualification tracking and reporting systems. The main production version of ASM is centrally hosted and supports operational Navy and Marine Corps forces worldwide, as well as industrial and administrative organizations. The ASM project team provides software design, testing, development, implementation, and life cycle support activities for the application.

SYSTEM ARCHITECTURE(S) / SOFTWARE TECHNOLOGIES	CURRENT DEPLOYMENT / UTILIZATION
SYSTEM ARCHITECTURES: Centrally-hosted, Web-based, Oracle Real Application Cluster. N-tier with multiple database, application, gateway and firewall servers. SOFTWARE TECHNOLOGIES: JAVA, JEE, Java Script, JSP Servlets, SQL, XML, AJAX, jQuery, CSS, HTML, Eclipse IDE, Google Web Toolkit, Hibernate.	Central server has 200,000 active user accounts. Peak user load approximately 2,000 users.

For the ASM program, perform the functions in paragraphs 4.4.1 - 4.4.6. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.4.1 Software Defect Fixes and Minor Modifications

For estimation purposes, assume four software releases per year with each comprised of 50 modifications (including fixes and cosmetic enhancements). The complexities of the modifications are as follows: 15 high, 20 medium, and 15 low.

4.4.2 Software Application Enhancements

For estimation purposes, assume one major software enhancement per year to extend ASM functionality. The contractor will be provided a software requirement specification in order to develop a cost and schedule estimate. For estimation purposes, assume the software project will be composed of 30 functional use cases to be prepared by the contractor; these will define the business rules which support the customer requirements and provide sufficient technical detail for the programmers to code the application. The use cases shall contain amplification of the user's requirements in order to support the software design process, and sufficient detail for the test engineers to construct and document the test cases. The use case complexities are as follows: 10 high, 15 medium, 5 low. The newly developed software must integrate with existing ASM functionality. The contractor will create design documents and submit them to the Government for approval. Software code shall be delivered incrementally for integration into the ASM application code line. The contractor will conduct monthly project reviews, periodic code reviews, and software demonstrations with the Government.

4.4.3 Software Architecture Modernization

Remove propriety software framework & re-architecture a modern, efficient, standard micro services architecture streamlining and

modernizing current ASM business rules and process functionality.

Provide upgraded user interface (UI).

4.4.4 Software Testing

For estimation purposes, assume four test events per year with each comprised of 50 defects. The complexities of the test cases are as follows: 15 high, 20 medium, and 15 low.

In addition, assume quarterly application regression test events for Central Processing Unit(CPU) patching comprised of 100 existing test cases and 100 reports.

4.4.5 Engineering/Cyber Security Support

For estimation purposes, assume 660 hours of technical documentation, 240 hours managing systems configuration including hardware/software lists and DoN Application and DADMS management, 60 hours of hard drive destruction, 480 hours removing/installing hardware, 400 hours system monitoring, 720 hours IAVA compliance management, 640 hours of new server builds, 480 hours of monthly Microsoft updates management and implementation, 1120 hours of STIG management, 200 hours of system backups, 720 hours of ACAS scan remediation, and 360 hours remediating cybersecurity vulnerabilities.

4.4.6 Project Management Support

For estimation purposes, assume two daily thirty-minute project meetings with minutes created and distributed electronically. Assume five annual project plans developed with earned value tracked and monthly reports prepared using Government provided templates.

4.4.7 Travel

Travel will be required in support of this effort as reflected in paragraph 4.14. All travel will be directed by the COR through TI's.

4.5 Task 5: Obsolescence Management Information System (OMISTM)

The OMISTM is a Navy-developed and owned web-based system in full production. The current major version is version 3. OMISTM provides obsolescence monitoring, integration of configuration and logistics data, and case resolution management of obsolescence issues for over 50 programs. The application is web based and is accessible from any DoD computer. The OMIS team provides all software design, testing, development, implementation, and support activities for the application.

SYSTEM ARCHITECTURE(S) / SOFTWARE TECHNOLOGIES	CURRENT DEPLOYMENT / UTILIZATION
SYSTEM ARCHITECTURES: Centrally hosted, Windows based server farm with failover SOFTWARE TECHNOLOGIES: Web-based application with SQL Server backend. .NET IDE, Visual Studio, Team Foundation Server or GitLab , C#, CSS, Bootstrap, JavaScript, HTML, JQuery, and .Net Core	Web application available to .mil users. 145 active user accounts

For the OMISTM program, perform the functions in paragraphs 4.5.1 through 4.5.3. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.5.1 Software Defect Fixes and Minor Modifications

For estimation purposes, assume Development is done using the Agile method, using sprints normally two-weeks in duration. Associated work is broken into sprint units. A sprint unit is equivalent to the development of one C# class with two methods of moderate complexity and four each inputs and outputs, coded, tested and working. A sprint unit for testing is equal to testing four development sprint units. For estimation purposes, assume 27 two-week sprints per year with each comprised of 70 development

sprint units and 35 test sprint units.

4.5.2 New Feature Releases

Using the same Agile method described in 4.5.1, for estimation purposes, assume 27 two-week sprints per year with each comprised of 70 development sprint units and 35 test sprint units.

4.5.3 Data Analytics and Research

For estimation purposes, assume two-month research increments, with deliverables on research project status due at the end of each increment. Research will include adapting well known methodologies to reach set research milestones, analyzing methods against results, while working in a small research team environment. May have to draft or review white papers and software documentation.

4.5.4 Travel

Travel will be required in support of this effort as reflected in paragraph 4.14. All travel will be directed by the COR through TI's.

4.6 Task 6: Nosis/Ship to Shore Data Exchange (S2DE) Support

The Nosis "paperless ship" is a web-based computing environment. It is composed of a central database and numerous software application-specific CSCIs that support various shipboard non-tactical functions including: administrative, maintenance, supply, watch standing, rigging, and training. Nosis is accessed through hull-specific home pages that are available to its crew(s). From the home pages, direct information such as electronic documentation may be accessed directly through the selection of unique links on each of the home pages. Access to the various Nosis software applications is made possible through a series of user-selected tabs located on each of the home pages. The Nosis team provides software design, testing, development, implementation and support activities for specific modules of the application, as well as government technical oversight for the complete suite of Nosis modules.

SYSTEM ARCHITECTURE(S) / SOFTWARE TECHNOLOGIES	CURRENT DEPLOYMENT / UTILIZATION
SYSTEM ARCHITECTURES: Multi-site virtual system consisting of Web-Based applications with multiple versions of the same product, with multiple SQL Server and Oracle databases. Server and F5 Network Traffic Manager Appliance. Submarine deployed web-based application modules. Modules hosted on program of record application systems on program of record LANs. Research and Test network which is rapidly reconfigurable to support various efforts. Contains heavy VM Ware virtualization with primarily Windows operating systems. SOFTWARE TECHNOLOGIES: Java, JEE, C#, ASP.NET, Ruby, Visual Basic Scripting and PowerShell Scripting	Multi-site virtual system has approximately 2,160 user accounts. Submarine deployed modules are deployed on all submarines. Each submarine has approximately 60 users.

For the Nosis/S2DE program, perform the functions in paragraphs 4.6.1 - 4.6.5. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.6.1 Software Defect Fixes and Minor Modifications

For estimation purposes, assume two software releases per year with each comprised of 30 modifications (including fixes and cosmetic enhancements). The complexities of the modifications are as follows: 5 high, 15 medium, and 10 low.

4.6.2 System Administration

For estimation purposes, assume annual maintenance of network integrity and connectivity, maintenance of software development

workstation configurations, ensuring compliance with information security policies and maintaining system backup and recovery. Ensure compliance through use of scanning tools and provide mitigation as required. For estimating purposes, assume 8 software development workstations, 8 IAVAs per month, and 2 STIGs per month.

4.6.3 Advanced Technical Support

For estimation purposes, assume one advanced technical assistance occurrence to resolve system performance issues related to software and hardware architecture. Assume 120 hours of support per occurrence.

4.6.4 Application Support

For estimation purposes, assume 1,200 advanced Application Support calls per year. Assume an average of 3 2 hours of support per occurrence.

4.6.5 Software Vulnerability Assessment

For estimation purposes, assume responsibility to conduct penetration testing and JAVA software code vulnerability analysis using government-provided automated tools as well as manual methods. Assume an average of 20 hours per week of support.

4.6.6 Travel

Travel will be required in support of this effort as reflected in paragraph 4.14. All travel will be directed by the COR through TI's.

4.7 Task 7: Weapon Systems Information Technology

The Weapon Systems Information Technology group comprises of multiple weapon systems used in both the Lightweight and Heavyweight Torpedo Navy Enterprise. This group is comprised of help desk support, Government Off-The-Shelf (GOTS) web application lifecycle development, and IA CS professionals to maintain the operational status of these weapon systems.

SYSTEM ARCHITECTURE(S) / SOFTWARE TECHNOLOGIES	CURRENT DEPLOYMENT / UTILIZATION
SYSTEM ARCHITECTURES: Centrally-hosted, Web-based, Microsoft SQL Server. N-tier with multiple database, application, gateway and firewall servers. Hosted on Virtual Machines in Navy Enterprise datacenters (NEDC). SOFTWARE TECHNOLOGIES: C#, Microsoft SQL Server, jQuery, Java Script, XML, CSS HTML, Microsoft Visual Studio IDE, Team Foundation Server, AGILE, Test Driven Development	Web applications available to .mil users and some foreign national users. Multiple web applications servicing over 1,000 concurrent users.

For the Weapon Systems Information Technology group, perform the functions in paragraphs 4.7.1 - 4.7.6. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.7.1 Software Defect Fixes and Minor Modifications

For estimation purposes, assume development is done using the AGILE method, using sprints normally of two-week duration. Associated work is broken into sprint units. A sprint unit is equivalent to the development of one C# class with two methods of moderate complexity and including Internal Validation and Verification (IV&V) testing with peer-reviews, and software documentation updates (to reflect enhancements). Assume 27 two-week sprints per year with each comprised of 70 development sprint units and 35 test sprint units.

4.7.2 New Software Releases

Using the same AGILE method described in 4.7.1, for estimation purposes, assume 27 two-week sprints per year with each comprised of 70 development sprint units and 35 test sprint units.

4.7.3 Software testing for capability Improvements

For estimation purposes, assume ad hoc testing to support software sprints. Execute test procedures write TRs for defects and deficiencies. For estimating purposes, assume 10 test cases and 20 test procedures per software sprint.

4.7.4 Application Support

For estimation purposes, assume 500 advanced Application Support calls per year. Assume an average of 30 minutes of support per occurrence.

4.7.5 Website Support

For estimation purposes, assume the designing, building, and maintaining of a small dynamic website with a database backend to government-provided requirements. Once established, assume an average of 2 days per week of support.

4.7.6 System Administration

For estimation purposes, assume annual maintenance of network integrity and connectivity, maintenance of software development workstation configurations, ensuring compliance with information security policies and maintaining system backup and recovery. Ensure compliance through use of scanning tools and provide mitigation as required. For estimating purposes, assume 18 Virtual Machine (VM) Servers (consisting of both web and database servers), 2 IAVAs per month, and 1 STIG per month.

4.7.7 IT Technical Writing

For estimation purposes, assume the generation of technical documents from software engineering artifacts such as use cases, requirement documents, sequence diagrams and help files. For estimating purposes, assume 200 use cases, 200 sequence diagrams, and 50 help files per year.

4.7.8 Travel

Travel will be required in support of this effort as reflected in paragraph 4.14. All travel will be directed by the COR through TI’s.

4.8 Task 8: Code 47 Cyber Security Engineering Support

For the IA/IO program, perform the functions in paragraphs 4.8.1 - 4.8.3. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

The IA functions are for various programs and projects internal and external to NUWC Keyport. These functions include preparing system accreditation documentation required by the Navy and/or DoD, evaluating security configurations of systems, and maintaining security configurations of production, development and test systems by applying/configuring security controls, and using appropriate tools to assess vulnerabilities of systems under test.

4.8.1 Cyber Security Support: System Security Configuration and Maintenance

For estimation purposes, assume full responsibility for maintaining the security configuration of proposed production system or production systems consisting of servers, routers, switches, applications and virtual environments. Security configurations are to be evaluated/maintained by the processing of IAVA's, STIG's and Critical Patch Updates through a rigorous configuration management process approved by higher authority.

4.8.2 Cyber Security Support: System Accreditation

For estimation purposes, assume responsibility for end-to-end preparation of a system accreditation package (System Accreditation Documentation) in accordance with the DoD Risk Management Framework requirements. Tasking includes assessing operating systems for compliance with DISA STIG's, completion of vulnerability scans and preparation of required supporting documentation. Systems to be accredited are comprised of various Microsoft servers, Linux variant servers and clients, routers, switches, software and possible cross domain solutions (CDS).

4.8.3 Travel

Travel will be required in support of this effort as reflected in paragraph 4.14. All travel will be directed by the COR through TI’s.

4.9 Task 9: Virtual In-Service Engineering System (VISE) Support

VISE is a Microsoft SharePoint Site Collection used within the Keyport In-Service Engineering Department for the storage, retrieval, processing, and collaboration of technical, organizational, and project/task information. It handles approximately 600 users and services customers internal and external to the organization.

SYSTEM ARCHITECTURE(S) / SOFTWARE TECHNOLOGIES	CURRENT DEPLOYMENT / UTILIZATION
SYSTEM ARCHITECTURE: SharePoint implementation is currently centrally hosted at NUWC Keyport in a server farm not under the control of the Software Application Development and Support team this contract will support. Server Farm administrative controls and settings are not managed or controlled by the government/contractor Software Application Development and Support Team, and are established by higher authorities external to NUWC Keyport. SOFTWARE TECHNOLOGIES: Microsoft Office and SharePoint 2010 and 2013, ASP.NET, C-sharp, CSS, HTML, JavaScript, jQuery, SharePoint Designer, Visual Studio Integrated Development Environment (IDE)	VISE Site Collections support 600 users in multiple locations.

For the VISE program, perform the functions in paragraphs 4.9.1 - 4.9.3. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.9.1 Application Modifications and Bug Fixes

For estimation purposes, assume 400 modifications per year including bug fixes, workflow modifications, web part modifications, and troubleshooting. Bug fixes, troubleshooting, and modifications will incorporate existing SharePoint software standards and methods using a variety of development tools.

4.9.2 Design and Management

For estimation purposes, assume 50 design enhancements per year to increase data management efficiency and design flow; design, code, test, debug and maintain SharePoint sites and pages in response to customer requests. Design and develop Graphical User Interface (GUI) features in response to customer requests.

4.9.3 Help Desk Support

For estimation purposes, assume 500 Help Desk calls per year. Calls cover a variety of issues that includes permissions, navigation, site creation, document retrieval and other SharePoint related issues. Assume 1 hour of support per occurrence.

4.9.4 Travel

No travel required.

4.10 Task 10: Code 40 Department Support

For Code 40 Department Support perform the functions in Section 4 of this PWS, and all sub sections. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.11 Task 11: Corporate IT Support

Corporate IT Support is the holistic operation and maintenance of Keyport IT infrastructures, which includes NMCI and RDT&E networks and services. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.11.1 Corporate Network Administration

Provide technical support in the installation, maintenance, operation, troubleshooting, upgrading and re-configuration of Keyport's corporate network components and cable facilities maintaining a 99.9% uptime not to include scheduled and approved outages. Estimate two (2) unclassified and three (3) classified environments, which include the following network scope:

- 300 Layer 2/Layer 3 devices
- 12 Wide Area Network (WAN) links
- Cisco Unified Communication Manger (CUCM) clusters
- Cisco Unity Connection (CUC) clusters
- Cisco Emergency Responder (CER) deployments
- 2200 VoIP phones
- 3 Cisco Identity Services Engine

Support functions include:

- Plan and perform regular scheduled maintenance on network infrastructure hardware and software including switches, routers, 802.1x system, Virtual Private Network (VPN) appliances, and VoIP components
- Troubleshoot complex enterprise routed IPv4 and IPv6 switched networks and VoIP utilizing modern network troubleshooting tools and sophisticated test equipment ensuring all equipment meets current DoD STIGs and IAVA requirements
- Apply 100% of IAVA's and STIGs to the system(s) by the due dates specified in published guidance unless delays are acceptable to the government for technical reasons
- Respond to trouble tickets within 60 minutes, acknowledge receipt via email, phone call, or site visit, perform the required function, and close out the tickets
- Estimate 20 tickets per day
- Install, troubleshoot, and provide preventative and corrective maintenance and repair of VoIP telephones and associated voice mail (Cisco Sys Inc.)
- Estimate 100 actions per year
- Provide VoIP support to include call manager, voice mail systems, CER, and Primary Rate Interface (PRI) gateway routers
- Estimate 175 actions per year
- Install, move, configure, maintain, monitor performance, test, diagnose, and resolve problems for all network hardware and software components
- Provide documentation related to any equipment change or modification; follow government owned Configuration Management plan
- Estimate 200 actions per year
- Update and maintain network engineering drawings and operation documentation.
- Estimate 30 actions per year
- Additional requirements include contractor assistance as needed in the administration and maintenance of Keyport's Intrusion Detection Systems (IDS) and Firewall systems to include the creation of IDS signatures and IDS event analysis along with the general configuration control and administrative maintenance of Keyport Firewall Systems.
- Provide monthly uptime metrics
- Execute projects related to upgrades and new capabilities
- Projects will be completed according to the agreed upon schedule with no more than minus 30-day variance
- Contractor will notify the government at a project variance of minus 15-days

4.11.2 Network Infrastructure Support

Provide technical support in the installation, maintenance, operation, troubleshooting, upgrading and re-configuration of Keyport's corporate network cable facilities. Estimate two (2) unclassified and three (3) classified environments and three (3) SCIFs, which include the following network scope:

Support functions include:

- Troubleshoot cable plant connectivity issues
- Perform copper and fiber optic installations and interconnectivity requirements, and various network modernization projects.

    - Estimate 24 modernization projects per year
- Respond to trouble tickets upon receipt, acknowledge receipt via email, phone call, or site visit, perform the required function, and close out the tickets.
    - Estimate 400 tickets per month
- Install, troubleshoot, and provide preventative and corrective maintenance and repair of VoIP telephones
    - Estimate 100 actions per year
- Provide support for move, add, and change to VoIP equipment and accounts
    - Estimate 175 actions per year
- Install, troubleshoot, and provide preventative and corrective maintenance and repair of the fiber optic cable system.
    - Estimate 8 actions per year
- Install, move, configure, maintain, monitor performance, test, diagnose, and resolve problems for all network hardware and software components.
- Provide documentation related to any equipment change or modification; follow government owned Configuration Management plan.
    - Estimate 200 actions per year
- Update and maintain network engineering drawings and operation documentation.
    - Estimate 30 actions per year
- Perform site surveys to determine scope and develop plans for network installs, moves, rip outs, and changes.
    - Estimate 20 actions per year
- Execute projects related to upgrades and new capabilities
- Projects will be completed according to the agreed upon schedule with no more than minus 30-day variance
- Contractor will notify the government at a project variance of minus 15-days
- Work in confined spaces, which are sometimes hazardous, may be required. This work includes, but is not limited to, manhole access to underground cable vaults and conduit/duct systems, that may require the use specialized safety equipment (i.e., portable gas monitors). Aerial cable work is required. This work will be performed in compliance with all Federal, State, Local, NUWC Division Keyport, and all applicable safety regulations.
- The installation of systems may require use of a leased vehicle, rental of special equipment to support emergent services, and minor parts to perform repairs, which includes, but is not limited to:
    - A vehicle with cable reel
    - Aerial cable lashing machine
    - Aerial lift

A variety of networking hardware/software will be used and supported under designated tasks. Representative products are identified in Table 4-1, Networking Environment.

Table C-2: Networking Environment

Layer 2/3 Devices	Wireless technologies
Modems	Unshielded Twisted Pair (UTP) Cable Testers
Terminal Servers	Transmission Control Protocol (TCP)/IP
Network Analyzers-Sniffers	Spectrum Analyzer
Optical Time Domain Reflectometer (OTDR)	Enterprise Monitors
Fiber Optic Cable Termination Equipment	Fusion Splicers
Cisco Access Control System	Cisco Identity Service Engine

Cisco Emergency Responder (CER)	Cisco Voice over IP (VoIP)
Keyport's networking environment consists of Ethernet and fiber optic installations. Performers shall be knowledgeable of the following:	
CAT5/6 Wiring (EIA/TIA 568A/B)	TDM based circuits
Ethernet (100Mbps – 10 Gbps)	Metro Ethernet (IP based circuits)
Wireless Intrusion Detection System (WIDS), Wired Equivalent Privacy (WEP), Access Point (AP)s	Simple Network Management Protocol (SNMP) Services
IPv4/IPv6	Bit Error Rate Tests
Type 1 Encryption	Cisco Net flow

Skills and/or certifications required:

- Fiber Optic cable installation and termination (CFOI certification)
- Ethernet cable installation and termination
- Current Comptia Security + and/or ISC2 SSCP (certification)
- Certified Network Associate certification and/or Current Cisco Certified Network Associate-Voice is required (certification)

4.11.3 Corporate VoIP Operations and Support

Provide holistic operation of Keyport's corporate VoIP system to include maintenance, troubleshoot, design and upgrade, and re-configuration ensuring compliance with Joint Interoperability Test Command (JITC) unified communications directives, DoD policy and mandates, and Defense Information Systems Agency STIGs. Maintain a 99.9% uptime for all VoIP components not to include scheduled and approved outages. The scope of this effort includes:

- Estimate 2000 VoIP users at Keyport and local detachments
- Estimate 400 VoIP users at Keyport's Hawaii and San Diego detachments
- Estimate 18 servers
  - 6 – ESX
  - 6 – Call Manager
  - 5 – Unity Voicemail
  - 5- CER
  - 1 – License sever
- Estimate 8 PRI routers
  - 10 – PRI lines
- Estimate 2500 VoIP phones

VoIP support includes the following tasking:

- Perform system updates and modernization
- Provide monitoring, reporting and backup/restoration services for all server functions and router configurations
- Ensure VoIP infrastructure is routinely scanned and patched
- Report compliance to Code 10 Information Systems Security Officer (ISSO) as required
- Assist in planning, design and configuration of new VoIP capabilities/upgrades
- Deploy government approved designs and new capabilities
- Apply 100% of IAVA's and STIGs to the system(s) by the due dates specified in published guidance unless delays are

acceptable to the government for technical reasons
- Provide monthly uptime metrics
- Execute projects related to upgrades and new capabilities
- Projects will be completed according to the agreed upon schedule with no more than minus 30-day variance
- Contractor will notify the government at a project variance of minus 15-days

4.11.4 IT Support Services

Keyport IT Support Services operates at a Tier 2 support level. Tier 2 IT support is defined as involving technical knowledge that is staffed by technicians who have refined troubleshooting skills beyond typical Tier 1 support level. Tier 2 personnel have an in-depth knowledge of corporate IT products and services, but not necessarily the administrator, engineer, or programmer who designed and created the product.

Personnel performing IT Support Services require a thorough understanding of the design, configuration, and deployment of Microsoft desktop operating systems, web browser configuration and troubleshooting, TCP/IP connectivity troubleshooting, access control and permissions, DNS client troubleshooting, desktop computer and peripheral configuration and troubleshooting.

IT Support Services incorporates operation of the corporate IT Support Desk, desktop and peripheral support, computer repair and baseline services, and Video Teleconference (VTC) operations, and Audio/Video/Streaming operations in support of command events. Table C-4 and C-5 lists required skills and a variety of hardware and software supported under this task. IT Support Services must meet the following government requirements:

- Operate during the core hours of 0600-1730 (M-F)
- Receive and resolve 80% of all tier 2 support requests
- Receive and assign all tier 3 customer support tickets
- Estimate 1000 tickets per month with a breakdown as follows:
  - 665 Tier 2 Customer Support tickets
  - 285 Tier 3 Escalated tickets
  - 20 Computer repair tickets
  - 30 VTC tickets/sessions
- Maintain less than 30 open tier 2 tickets
- Track all tier 3 tickets to resolution coordinating with appropriate teams
- Perform customer satisfaction surveys on a minimum of 10% of the overall IT support incident requests daily
- Advocate for the customer through ticket resolution and closure for all tier 3/escalated tickets

4.11.4.1 IT Support Services

- Operate and monitor on-site Tier 2 IT Support operations resolving questions related to Keyport user support with a minimum “first call resolution” goal of 80%. For the purposes of this PWS, First Call Resolution is defined as a Customer's inquiry or problem is resolved in one call, without escalation, eliminating further calls by the IT Support or customer to reach a solution
- Assist the Activity Contract Technical Representative in the ordering and delivery on NGEN/NMCI services including user accounts, computers, software, and peripherals
- Troubleshoot NGEN/NMCI user accounts, computer, and software delivery issues
- Enter and track all requested actions in Government provided tracking system
- Provide monthly reports on number of actions performed including time to resolve
- Track and report weekly on first call resolution and escalated tickets by call type
- Record, assign, and track all trouble calls that come into the IT Support using designated call-tracking software
- Escalate or forward trouble tickets that cannot be resolved to the appropriate team
- Acknowledge customer tickets within 30 minutes of receipt
- Monitor IT systems and services and notify the appropriate team or individual when a failure occurs on one or more of the following services/applications:
  - VPN
  - Networking Services
  - Customer Open Calls and or un-acknowledged trouble tickets
  - Corporate Applications and or Services accessibility
- Document and/or create procedures and processes used to support operation and monitoring of IT Support Services.

    - Estimate 20 procedures/processes per year
- Create and provide monthly metrics that reflect the workload and level of effort within IT Support Services.
- Manage Active Directory domain users including account creations, deletions, and modifications.
    - Estimate 30 actions per month
- Maintain digital reader board information and configuration.
    - Estimate 100 actions per year
- Manage and schedule the daily operation of Keyport's corporate Video Teleconferencing systems
- Schedule, setup, and troubleshoot unclassified and classified corporate VTC sessions
- Maintain VTC room access and usage logs.
- Provide monthly metrics on VTC's total number of sessions including successful and unsuccessful events
- Provide presentation support for command functions/events to include:
    - Video capture and streaming
        - Estimate 10 events per year
    - Setup/teardown of microphone and PA systems
        - Estimate 20 events per year
- Operation/maintenance/troubleshooting of video walls and reader boards

4.11.4.2 Desktop and Peripheral Support

Provide analytical and technical on-site support for the operations of desktop/laptop computers, workstations, and peripherals on corporate hardware within unclassified and classified environments.

Design, develop, and maintain installations of a variety of client operating systems including, but not limited to activities associated with the investigation of new operating systems, deployment and installation techniques and options, the maintenance and updates for new and existing operating systems, and the configuration of the many different components of the workstation operating system to provide for reliable and stable integration into the Keyport environment.

Support includes:

- Acknowledge customer tickets within 30 minutes of receipt
- Install, maintain, and troubleshoot user application software and system configurations
- Develop and maintain configurations for a variety of client computing systems, such as workstations, laptops, and handheld computers baselines meeting all current DoD STIGs and IAVA requirements
- Ensure 100% of IAVA's and STIGs are applied to the system(s) and system baselines by the due dates specified in published guidance unless delays are acceptable to the government for technical reasons
- Perform scanning/remediation of domain and non-domain assets using approved DoD tools
- Remediate vulnerabilities and/or develop mitigation strategies
- Troubleshoot desktop connectivity issues, DNS configurations, and IP addressing conflicts
- Update system and office automation configurations, in accordance with the baseline to current standards, software versions/releases, and solve user initiated configuration problems
- Provide customer support via the network, the telephone, or personal on-site visits to identify, troubleshoot, analyze, and resolve desktop systems and/or corporate application errors
- Create and maintain server based print queues
- Utilize automated centralized management techniques for software deployment, maintenance, and configuration
- Provide troubleshooting support and training on defined corporate software and office suite baselines (such as MS Office, Windows Operating System, and SharePoint)
- Provide conference room support including Personal Computer (PC) setups, PC projection and PC sound including remote collaboration tool configuration and setup
    - Estimate 5 per month

4.11.4.3 Computer Repair and Baseline Services

Provide support for desktop and laptop computers, printers, and monitors. Support includes:

- Acknowledge customer tickets within 30 minutes of receipt
    - Estimate 100 tickets per month maintaining an estimated 1100 PC's, monitors, 100 laser/inkjet printers.
- Perform PC workstation installation, troubleshooting, preventative, and corrective maintenance of Government controlled

RDT&E computing hardware and associated peripherals.

- Identify hardware problems and recommend disposition to the customer if spare stock is not available.
- Evaluate hardware/software compatibility.
- Provide hardware upgrade and replacement recommendations.
- Provide customers with estimated upgrade/repair costs and turn-around time. Prioritize workload based on emergent customer requirements.
- Manage, maintain, and deploy DISA Secure Host Baseline (SHB) Operating Systems in accordance with the current SHB schedule.
- Ensure 100% of IAVA's and STIGs are applied to the system(s) and system baselines by the due dates specified in published guidance unless delays are acceptable to the government for technical reasons.
- Design, create, and maintain standardized client images for deployment purposes.
- Develop, maintain, and operate automation tools for the deployment of approved baseline images.
- Provide monthly metrics on number of systems that were base-lined and Mean Time to Repair with a goal of four (4) business day turnaround.
- Retain replaced parts to be reutilized as spares. Hardware covered under warranty shall be shipped to the vendor and the customer shall be notified on return of the item.

A variety of hardware and software will be used in tasks 4.11.4. Representative products are identified in Table C-3, Helpdesk Services.

Table C-3, Helpdesk Services

Email Clients	Databases
Data at Rest Technologies	Graphics Programs
Linux OS	Project Management Software
Windows Desktop OS	Query /Reporting Software
Windows Server OS	Web Tools
Microsoft Office Tool Suite	Windows Active Directory
Remote Desktop Control Software	Web Hyperlink Tools
Desktop and laptop computer systems	Networked and non-network printers
Networked and non-network scanners	Smartcard authentication
Software Deployment Technologies	Portal Administration Services
ACAS/Vulnerability Scanners	System/Network Monitoring tools (Orion)
VoIP Configuration	Virtualization

Minimum or better skill set required for Customer User Support (IT Support Services):

- Current CompTIA Security + and/or ISC2 SSCP
- Current Microsoft Desktop Operating System Certification
- Understanding of Virtual Private Networking
- Understanding of Web Proxy services
- Understanding of Data at Rest solutions

4.11.5 Server Administration

Keyport corporate IT consists of several server farms that exist locally, at various detachment sites, and at CCSP Federal Risk and Authorization Management Program (FedRAMP) Impact Level Four/Five (IL4/5) environments. Server support requires specialized skills and experience in the operation of large geographically dispersed IT infrastructures. These infrastructures may be network connected or isolated as a stand-alone enclave.

Server support will consist of providing analytical and technical on-site support for the operations of Windows/Linux based servers and storage. Estimate four (4) unclassified environments and two (2) classified environments with the following estimated total server/storage count:

- Physical Servers: 80
- Virtual Servers: 300
- Storage Arrays: 15

The contractor shall attempt to achieve 99.5% availability for all Keyport Corporate systems not to include scheduled and approved outages. Requirements include the operation and maintenance of the corporate servers/systems, listed:

- Internet Information Services
- Microsoft SQL Services
- Team Foundation Services
- Servers using Microsoft Server and Linux Operating Systems
- System Management
- Software Update Services
- Load-Balancing/Clustering Services
- SharePoint Services
- Server Certificate Services
- Virtual Application Services
- SNMP Management/Monitoring tools
- HP EVA, MSA, 3PAR, NetApp Storage Arrays
- Virtualization Services
- Microsoft Active Directory
- ACAS
- Host Based Security System (HBSS)
- Enterprise Backup software
- Data at Rest (DAR) Technologies

Provider's responsibilities shall include the following services:

- The contractor shall respond to assigned trouble-tickets calling the customer within 30 minutes of receipt to acknowledge.
  - Estimate 400 tickets annually
- Plan and coordinate installation, testing, troubleshooting, operation, and maintenance of hardware and software systems for all corporate servers/systems.
- Maintain corporate server Operating System (OS) baselines meeting all current DoD STIGs and IAVA requirements.
- Plan and schedule the installation of new and modified hardware/software, allocating system resources, managing accounts, network rights, and access to systems and equipment.
- Perform server backups to provide for system restoration, file and database recovery, and disaster recovery.
  - Estimate 25 backup routines performed nightly
- Validate backups periodically to ensure restoration success.
  - Estimate a 10% sampling monthly to ensure full restore capabilities
- Document, recover, reload, and restore files, server volumes, and databases as required to provide immediate user access to

required data
    - Estimate 30 recoveries annually
- Implement and utilize cybersecurity procedures and tools.
- Resolve hardware/software interface and interoperability problems ensuring system functionality, integrity, and efficiency
- Monitor server and site Secure Socket Layer (SSL) certificates and request and install as needed.
    - Estimate 20 DoD SSL requests annually
- Maintain IAVA requirements through the installation and integration of system patches, updates, and enhancements per Government policy.
    - Estimate 52 patch cycles per year
- Support administration of the network's HBSS system to include ePolicy Orchestrator, McAfee Agent, ePolicy Auditor, Rogue System Detection, Asset Baseline Monitor, Host Intrusion Prevention, and the Super-Agent in accordance with the STIG.
- Provide support for enterprise Storage Area Network (SAN) including the configuration and provisioning of storage.
    - Estimate 30 actions weekly
- Operate and maintain corporate Data at Rest (DAR) solution to include application locking and key recovery.
    - Estimate 700 devices
- Provide bi-weekly reports supporting IAVAs.
- Document and/or create procedures and processes used to support operation and monitoring of the Server Support functions.
    - Estimate 20 annually

Provide resource utilization and capacity planning support, which includes:

- Baseline utilization of server/system resources (CPU), memory, storage space, backup capacity)
- Monitoring of the server/system resources monthly to identify utilization/consumption trends, and projecting when resource utilization/consumption will be such that delivery of services by the servers/system falls below acceptable performance levels in accordance with Government and or industry specifications
- Operate and maintain Corporate Host Based Security System meeting all DoD requirements and guidance.
- Assist with the daily operations and maintenance of Microsoft SQL clustering solution
- Validate nightly backup routines completed satisfactory; correct backup errors as needed
- Assist with the application of security patches and planned upgrades
- Apply 100% of IAVA's and STIGs to the system(s) by the due dates specified in published guidance unless delays are acceptable to the government for technical reasons.
- Create, manage, and maintain technical drawing and documentation sets for the execution of this task
- Provide monthly uptime metrics via government provided monitoring system
- Execute projects related to upgrades and new capabilities
- Projects will be completed according to the agreed upon schedule with no more than minus 30-day variance
- Contractor will notify the government at a project variance of minus 15-days

A variety of hardware and software will be used in tasks 4.11.5. Representative products are identified in Table C-4, Server Environment.

Table C-4: Server Environment

VMware ESX/VSphere	HP Blade Systems
Clustering Services	HP 3PAR Storage Arrays
Microsoft Internet Information Services	HP Continuous Access
NetApp Storage Systems	Linux Operating Systems
Microsoft SQL Services	Brocade Fiber Switches

Veritas Backup Suite	Brocade SAN Extension Switches
SharePoint Services	HBSS
Storage Area Network	Software Update Services
DoD SSL certificates	Smartcard Authentication
Active Directory Services	Windows Server OSs
DNS/DHCP	SCCM
TFS	WDS

Minimum or better skill set required for Server Support in accordance with DoD Cybersecurity Workforce Requirements:

- Current CompTIA Security + and/or ISC2 SSCP
- Current Server and/or virtualization certification

4.11.5.1 SharePoint Services Operations
Keyport utilizes a large SharePoint environment that supports corporate operations through the hosting of numerous sites, lists, and document libraries. SharePoint Services Support consists of the operation and maintenance of SharePoint farms, three (3) unclassified and two (2) classified. Locations for the farms are local to Keyport and hosted within the Navy Portal, iNAVSEA/iNAVY.

In general, the scope of Keyport's SharePoint consists of:

- 12 servers
- Estimate 1700 web sites
- Estimate 40 databases
- Estimate 2 TBs of data
- Estimate 5000 users throughout Keyport and NAVSEA

In alignment with higher DoD guidance, it is expected that Keyport will eventually migrate all SharePoint to the iNAVSEA/iNAVY portals or commercial cloud offerings at which time SharePoint Services Operations and Maintenance would be limited to the SharePoint application and eliminate the management and support of physical or virtual servers.

The contractor will provide SharePoint Services Support to include:

- Acknowledge customer tickets within 30 minutes of receipt
- Maintain a minimum 99.5% uptime for Keyport hosted SharePoint environment
- Operation, maintenance, patching, upgrades, backup and restore of all physical and virtual servers within the various enclaves
- Monitoring and performance tuning
- Provide quarterly reports on storage growth using total available storage to allocated storage for all enclaves
- Create, manage, and maintain technical drawing and documentation sets for the execution of this task
- Operation, maintenance, patching, upgrades, backup and restore of the SharePoint applications within the various enclaves
- Monitoring and performance tuning
- Quarterly clean-up/purging of SharePoint sites that are unused or no longer needed
- Develop and/or update processes/work procedures
- Assist government in out-year planning and design upgrades/changes

- Communicate issues, work plans, and changes to government for customer notifications
- Provide monthly uptime metrics
- Apply 100% of IAVA's and STIGs to the system(s) by the due dates specified in published guidance unless delays are acceptable to the government for technical reasons.
- Execute projects related to upgrades and new capabilities
- Projects will be completed according to the agreed upon schedule with no more than minus 30-day variance
- Contractor will notify the government at a project variance of minus 15-days

4.11.5.2 Storage Area Network (SAN) Operations

Keyport utilizes large storage volumes over several SAN environments to support server virtualization, general data stores, and backup capabilities. The SAN environments leverage Fiber Channel (isolated from the data networks) and iSCSI protocols over the data networks to support the various missions and user needs. The scope of SANs at Keyport is as follows:

- 3 unclassified enclaves using FCP
- 2 classified enclaves using FCP and iSCSI
- Estimate 2PB of storage
- Estimate 250 Logical Unit Numbers (LUNS)
- Estimate 14 core Fabric switches
- Estimate 12 edge Fabric switches
- Estimate 15 storage systems

The contractor will provide the following SAN Operations Support:

- Acknowledge customer tickets within 30 minutes of receipt
- Operation, maintenance, integration, and tuning of Keyport's corporate SANs and storage systems
- Ensure compliance with DoD/DoN Policy and mandates including IAVM and STIGs
- Apply 100% of IAVA's and STIGs to the system(s) by the due dates specified in published guidance unless delays are acceptable to the government for technical reasons
- Maintain 99.99% availability not including scheduled and approved outages
- Provide monthly uptime metrics
- Monitor and tune the performance of SAN and storage systems
- Provide quarterly reports on storage growth using total available storage to allocated storage for all enclaves
- Provide monthly reports on SAN port utilization for all enclaves
- Provide monthly reports on SAN and storage system availability
- Create, manage, and maintain technical drawing and documentation sets for the execution of this task
- Research and provide recommendations for technology upgrades and/or configuration changes
- Execute projects related to upgrades and new capabilities
- Projects will be completed according to the agreed upon schedule with no more than minus 30-day variance
- Contractor will notify the government at a project variance of minus 15-days
- Current SAN and Storage systems consist of:
- Brocade and Cisco fabric switches
- HP and NetApp storage systems

Minimum required qualification and skillset:

- 5 years' experience with the operations, maintenance, and integration of SANs (fabric and switching technologies) utilizing Fiber Channel and iSCSI protocols
- 5 years' experience with the operation, maintenance, and integration of large storage array systems, the application of various RAID levels, and assignment and documentation of LUNS.

4.11.5.3 Vulnerability Management Operations

Keyport utilizes a robust Vulnerability Management process to ensure network connected systems remain compliant and in alignment to IAVA, Information Assurance Vulnerability Bulletins (IAVB), DISA STIGS, Computer Tasking Orders (CTO), and applicable National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls.

Vulnerability management includes monitoring, scanning and patching of Windows and Linux desktop operating systems across NUWC Keyport IAW Keyport comprehensive vulnerability management plan. The tasking applies to all Keyport network

connected enclaves and may include transferring of patching and Group Policy Object packages to stand-alone enclaves for deployment. Assume the following scope:

- Two (2) classified network connected enclaves
- One (1) stand-alone classified enclave
- Two (2) unclassified network connected enclaves
- One (1) stand-alone unclassified enclave
- 2000 endpoints

For this tasking the contractor will provide the following support:

- Acknowledge customer support requests within 30 minutes of receipt
- Provide end-to-end POA&M management for all identified risks
- Execute weekly vulnerability management program per government provided processes
- Perform routine scanning of all classified and unclassified network connected enclaves
- Maintain deployable laptop scanners for use in stand-alone enclaves
- Maintain automated imaging and patch deployment tools
- Analyze, build, and test a variety of software patches for deployment to network connected systems
- Deploy tested patches via automated deployment tools
- Troubleshoot and repair failed deployments and/or patch installs
- Analyze, implement, and test Microsoft Active Directory Group Policy Objects to meet DISA STIG requirements and other mandates or guidance
- Communicate weekly patching plans per government provided processes
- Report compliance IAW comprehensive vulnerability management plan
- Work with Cybersecurity Branch to create POAMs for any findings that cannot be resolved
- Create, and capture workstation, and server images that can be automatically deployed
- Maintain STIG compliant workstations, and server images with current software, and updates, as required in government provided processes
- Apply 100% of IAVA's and STIGs to the system(s) by the due dates specified in published guidance unless delays are acceptable to the government for technical reasons

4.11.6 Cybersecurity Services

Code 104 provides numerous aspects of Cybersecurity Support representing Command interests and reporting as well as significant direct support to system owners and end-users. These areas include various aspects of Cybersecurity (CS) compliance and CS customer support areas. Support areas addressed by this section include oversight, support, and validation for information systems Assess and Authorize efforts; oversight of system and data access approvals, providing CS technical support and guidance developing CS policy implementation plans; IAVM/Vulnerability Remediation Asset Management execution and reporting; Communication tasking orders compliance; ensuring Command CS defense-in-depth strategy, compliance, and investigating misuse of critical IT; the CSWF Program , ensuring compliance with Navy Cyber Defense Operations Command directives.

4.11.6.1 RMF Verification and Validation

Perform independent Verification and Validation as Fully Qualified Navy Validators for NUWC Keyport RMF packages.

- Verify technical compliance through automated scans
- Verify technical compliance through manual reviews
- Verify non-technical compliance through manual review
- Validate Plan of Actions and Milestones (POA&M)
- Ensure traceability between Findings and POA&M
- Verify required documentation
- Execute eMASS Validation Procedure entries
- Create Security Assessment Plans (SAP) 4.11
- Create Certification Determination Letters
- Represent system throughout the approval process
- Perform Annual Review and document results
- Attend CCB meetings
- Support re-accreditation efforts

- Support Risk Management Framework (RMF) Transitions
- Execute validation projects
- Projects will be completed according to the agreed upon schedule with no more than minus 30-day variance
- Contractor will notify the government at a project variance of minus 15-days
- Estimate 6000 hours or three FTE for this effort. Personnel must be FQNV IAM Level III qualified in accordance with the DoD 8570.1-M.
- Estimate 10 new packages annually
- Estimate 20 Interim Authority to Test packages annually
- Estimate 65 annual package reviews

All A&A packages shall be managed and maintained at a compliance level of 90% at all times. Compliance is measured by the following elements:

- All Use Case I, II, III, IV / Change Requests shall be processed once the need is identified
- All approved Use Case I, II, and III requests shall be processed and updated in eMASS monthly
- All approved Use Case IV requests shall be processed and updated in eMASS quarterly
- The government shall be notified of any issues that lead to possible delay in meeting these expectations
- A&A Package Lifecycle Support
- Perform cybersecurity support and processing functions as needed per government provided processes
- Routine CM request approval and processing
- Routine CM request approval
- Routine CM request quality assurance
- Routine A&A package maintenance

4.11.6.2 Cybersecurity Support

Perform cybersecurity support functions as needed per government provided processes, to include:

- Routine SAAR processing
- Requesting, issuing, and performing pin resets for alt access tokens
- Execution of the Message Transfer Agent process
- Media Transfer Agent (MTA)
- CSWF
- Technical Documentation
- Auditing and Inspection Preparation
- Vulnerability Management
- Information Systems Security Officer (ISSO)
- CCRI/CCORI Preparation

4.11.6.2.1 System Authorization Access Request Navy (SAAR-N) Processing

- Be delegated the authority to process and sign SAAR-N forms on behalf of the Information Assurance Manager (IAM)
- Assist in SAAR-N routing as necessary to lead to successful completion
- Perform verification that all required fields of the SAAR-N form are completed and signed as appropriate
- Maintain file depository of all completed SAAR-N forms to meet audit requirements
- Manage/approve user account requests in accordance with local requirements and established processes
- Perform annual audits on all SAAR-Ns to ensure compliance for all accounts and that all SAAR-Ns are accurate and up to date
- Routine SAAR processing
- Process completed SAARs within two workdays, follow up within 1 day on incomplete/missing SAARs, and weekly thereafter until completion.
- Process SIPR Token requests with 2 workdays, and notifies users of tokens ready for issue within 2 workdays, and follow up weekly thereafter until completion.
- Provide monthly metrics on token and SAAR processing time

4.11.6.2.2 DoD "Tokens" Public Key Infrastructure Program Submitting Trusted Agent (STA)(NIPR/SIPR)

The contractor shall perform the duties of the STA for the DoD Public Key Infrastructure Program for the issuance of the Alternate

Token (Alt-Token) and the Alternative Login certificate.

- As the STA, the contractor shall ensure control of issued Alt- tokens for local holders of secondary accounts (i.e., .adm and/or.dev accounts).
- The contractor shall gather and forward subscriber registration information to the Hardware Token Registration Authority (HTRA) at Space and Naval Warfare Systems Command (SPAWAR) System Center (SSC) Atlantic.
- The contractor shall maintain an ongoing list of users with Alt-tokens along with a copy of the signed DoD Public Key Infrastructure (PKI) Acknowledgement of Responsibilities for Alternate Token and Certificate form.
- The contractor shall verify the identity of each System Administrator/Developer (SA/DEV) prior to issuing the Alt-tokens.
- The contractor shall recover the Alt-token from the SA/DEV when they are transferred, reassigned or otherwise replaced, and return the Alt-token to the HTRA in accordance with the procedures contained in the US Navy Alt-Token Standard Operating Procedures (SOP).
- National Security Systems (NSS) Public Key Infrastructure (PKI) Trusted Agent (TA) for SIPR Tokens.
- Be delegated the authority to perform actions on behalf of the Registration Authority (RA)
- Perform subscriber validation, registration, identity verification, and token/PIN information distribution
- Perform token creation, issuance, revocation, suspension, restoration, pin reset, failure reporting, and return
- Maintain all audit information such as custody logs, signed DD Form 2842s locally, and forward to the RA as required
- Abide by all applicable requirements of the DoD Registration Practice Statement (RPS)

4.11.6.2.3 Media Transfer Agent Process Execution

- The contractor shall support the MTA – Data Write program to ensure IA Compliance
- The contractor shall support the identification, documentation, tracking, and reporting of Program Forms, Systems, Media Inventory, and MTA Request Forms.
- The contractor shall support the creation and modification of briefing materials, issue papers, point papers, ad hoc reports, as required, and be proficient in the use of Navy standard office automation products including Microsoft Word, PowerPoint, Excel, Project, Access as well as Microsoft SharePoint
- Contractor shall provide progress, status and management report 2 days after end of each month
- Contractor shall provide quarterly audit report 5 days after end of each quarter
- Contractor shall provide semiannual audit report 5 days after end of the 2nd and 4th quarter

4.11.6.2.4 Cybersecurity Workforce Support

- The contractor shall support the Information Assurance (IA) & CSWF to ensure IA Compliance
- The contractor shall support the identification, documentation, tracking, and reporting of CSWF certification status and continuing education
- The contractor shall support the creation and modification of briefing materials, issue papers, point papers, ad hoc reports, as required, and be proficient in the use of Navy standard office automation products including Microsoft Word, PowerPoint, Excel, Project, and Access
- The Contractor shall provide ongoing records of CSWF member’s status (approx. 350 CSWF members)
- Provide quarterly proportional audit of status and accuracy (25% per quarter) 15 days after end of each quarter

4.11.6.2.5 Auditing and Inspection Preparation

- Develop checklists to use for assessments based on established guidance
- Conduct an internal review of Code 1043 directives, processes, and SOPs
- Quarterly package audits shall be conducted to ensure 100% compliance to include all changes to date
- Ensure cybersecurity documentation is current and accessible including OQE
- Identify lessons learned from other Sites and incorporate into our readiness process
- Develop milestones for inspection readiness and regularly report on status

4.11.6.2.6 Vulnerability Management Support

- The contractor shall perform vulnerability scans using DoD approved tools
- The contractor shall maintain awareness of DoD IA Vulnerability Management deadlines, announcements, applicability, and plan responses.
- The contractor shall research and document remediation strategies for vulnerabilities, build custom reports for data calls.
- The Contractor shall perform testing and analysis of IA controls and secure configuration using the ACAS, DISA STIG,

STIGviewer, SCAP Compliance Checker, and associated tools.
- The contractor shall prepare for Command Cyber Readiness Inspections (CCRI), Cyber Security Inspections (CSI), and other network inspections by developing documents such as standard operating procedures (SOP) and associated diagrams as directed.

4.11.6.2.7 Information Systems Security Officer (ISSO) Support

- Ensure the network, site, system, or application information system is certified and accredited.
- Provide guidance and recommendations for secure configurations
- Perform monthly scan reviews
- Perform quarterly STIG reviews
- Support C&A / A&A efforts
- Assess and support ensuring information systems are operated, used, maintained, and disposed of in accordance with security policies and practices.
- Verify security policies and safeguards on all personnel having access to the information systems.
- Continuous monitoring as mandated in step six of RMF.
- Conduct periodic reviews to ensure compliance with the accreditation and/or certification support documentation package. Perform/review Vulnerability Assessments, STIGS, Inventories, eMASS POA&Ms
- Support Configuration Management (New adds, Baselining and Baseline change management).
- Initiate protective or corrective measures to maintain security on information systems.
- Provide regular dissemination of Cybercomm TASKORDS, IAVAS, acknowledge receipt of IAVAS, Answer Data Calls, Reviews Vulnerability assessments and STIGS and directs corrective measures as required, Coordinates with ISSEs, VMs, and ISSMs
- Ensure support to information assurance vulnerability management (IAVM) requirements and ensure security patches are installed, as appropriate
- Report security incidents to the ISSM and/or cognizant NOA/DAA in accordance with policy and procedures.
- Resolve IT Support tickets
- Acknowledge support tickets within 30 minutes of receipt
- Develop processes to support overall cybersecurity program
- Assist with local policy development.
- Required Qualifications
    - Cybersecurity (CSWF) qualification required
    - System Analyst Level I
- One (1) of the following commercial certifications:
    - CompTIA Security + (SY0-401)
    - International Information Systems Security Certification Consortium (ISC2) Certified Authorization Professional (CAP)
    - CompTIA Advanced Security Practitioner (CASP)
    - Information Systems Audit and Control Association (ISACA) Certified Information Security Manager (CISM)
    - ISC2 Certified Information Systems Security Professional (CISSP)
    - Global Information Assurance Certification (GIAC) Security Leadership Certification (GSLC)

4.11.6.3 CCRI/CCORI Preparation Support

The contractor shall perform annual Command Cyber Readiness Inspection (CCRI)/Command Cyber Operational Readiness Inspection (CCORI) assessment, at Keyport proper, with the goal of improving cyber posture to by conducting annual independent assessments of Non-Secure Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), Defense Research Engineering Network (DREN)/Secret Defense Research Engineering Network (SDREN) and RDT&E enclaves. The contractor shall validate compliance with the DISA CCRI/CCORI Computer Network Defense (CND) Directive Guide.

The contractor shall be proficient in technology areas for which they are assessing and hold current applicable computing environment certifications. Areas of emphasis are as follows:

- Vulnerably Management and Compliance Assessment to include, Vulnerator, Vulnerability Remediation Asset Manager (VRAM), ACAS, Security Content Automation Protocol (SCAP)
- Operating Systems to include: Windows Servers, Windows Clients, Unix, Red Hat, CentOS
- Boundary Defense to include: Switches, Routers, Firewall, IDS Demilitarized Zone (DMZ)
- Endpoint Encryption Solutions, to include, but not limited to, Host Based Security System (HBSS), Host Intrusion

Prevention Systems (HIPS)
- Database administration and security for SQL and Oracle
- Web Services security for IIS, Apache, and Proxy server
- Social Media Security
- Network Configuration and Security
- Remote Access Security
- Port Security
- Data at Rest security
- Traditional Security
- Physical security, to include Cabling Infrastructure
- Wireless Security
- Mobile Device security
- VoIP Security
- VTC Security

As part of the assessment, the contractor shall ensure that enclave boundaries (e.g., crypto boundary, certification boundary, classification boundary) are clearly identified.

As part of the assessment, the contractor shall ensure requirements of DISA STIGs/Security Requirements Guides (SRGs) have been implemented across each enclave.

The assessment team will be led by a certified DODIN Readiness and Security Inspections (DRSI) member with a thorough understanding of the CCRI/CCORI frameworks.

Members of the contractor assessment team shall comply with DoD Directive 8140.01 and DoD 8570.01-M and meet the clearance investigative requirements:

- Qualified IAM level II and Level III
- Qualified IAT level II and Level III
- Possess DoD SECRET Clearance, with T-2 eligibility
- Additionally, HBSS evaluators will possess DOD Top Secret Clearance, with IT-3 eligibility

The contractor shall be knowledgeable with the DoD regulations:

- DISA Command Cyber Readiness Inspection (CCRI) Computer Network Defense (CND) Directive Guide
- DoDI 8500.01, Cybersecurity, 14 Mar 14
- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology, 12 Mar 14
- Communications Tasking Orders (CTOs), Warning Orders (WARNORDS), Task Orders (TASKORDs), Operations Orders (OPORDs) and Fragmentary Orders (FRAGOs)

The contractor shall develop a detailed and comprehensive report on findings identified and provide an analysis of the security posture of the enclaves to the Government no later than 30 days after the completion of the assessment. The report shall include recommended countermeasures, risk mitigations, and security posture improvements. In addition, at the end of the assessment period, the contractor shall provide an out brief to Keyport IT Management on their findings.

In the event a significant finding, i.e.,failure of an existing security control, data exposure or data loss is identified, the contractor shall notify the Government immediately..

It is estimated that a total of 2000 hours will be required to execute this tasking. The annual assessment will occur over a two (2) week period within the base and option years as agreed upon with the NUWC Keyport ACIO. Remaining hours will be used to provide guidance and assistance in correcting assessment issues.

4.11.7 Corporate Process Automation Support
Follow Navy initiatives, Federal regulations, and Corporate Application Team (CAT) processes and guidelines.

This requirement includes:

- Support SharePoint Services and sites on the Seamless Warfare Center (SWC) including creating new sites, and providing access to the sites.
- SharePoint development of sites/functionality using the current Visual Studio Integrated Development Environment (IDE), SharePoint Designer, ASP.NET, Cascading Style Sheets (CSS), HTML, JavaScript, JQuery
- Ability to perform lifecycle management, program using agile methodology, and understanding and ability to use and database analytical skills.
- Building Web Front ends, sandboxed solutions with Visual Studio and C#, event receivers.
- SharePoint troubleshooting skills with understanding of Unified Logging Service (ULS), SharePoint Architecture, European Computer Manufacturers Association (ECMA) Script, JQuery JavaScript, Custom Lists, Data Form Web Parts.
- Execute projects related to new applications or modifications
- Projects will be completed according to the agreed upon schedule with no more than minus 30-day variance
- Contractor will notify the government at a project variance of minus 15-days

4.11.7.1 Corporate Web Support

The contractor shall provide the following web support utilizing such software as Microsoft Office, Hyper Text Markup Language (HTML), Microsoft SharePoint Designer, Microsoft .NET development tools, and Microsoft SharePoint.

- Design, create, and maintain NUWC Division Keyport's intranet and internet web sites for numerous internal and external links and sites
- Implement new technologies as they become available that are Government approved.
- Implement inter-agency and other Federal requests and mandates for changes to existing web sites that are Government approved
- Administer Web Servers using Microsoft Internet Information Services (IIS) Servers and various web technologies listed in Table C-5
- Design, maintain, and install Web pages on the Intranet
- Provide training materials and procedures related to web pages
- Prepare help guides for publication on the Intranet
- Design, develop, and maintain client systems for remote access/mobile computing activities, which include host and client components
- Document procedures and processes developed, supplied, or modified for customer support and problem resolution

Software engineering and developmental tools used for development and maintenance of Corporate Applications and Web Sites applicable to tasks 4.11.7 are identified in Table C-5, Application/Database Environment.

Table C-5, Application/Database Environment

Microsoft Visual Studio Integrated Development Environment	Databases
Microsoft.Net Compact Framework	Graphics Programs
Microsoft Team Foundation Services	Project Management Software
Microsoft Active Directory	Query/Reporting Software
Microsoft Reporting Services	Microsoft Visual Basic
Microsoft Analysis Services (OLAP)	Visual Studio Team Systems
Domain Name Services (DNS)	Adobe Flash/Design Suite
Microsoft SharePoint Development	JavaScript and JQuery
Microsoft SharePoint Designer	Web Design in SharePoint
ASP.NET	Cascading Style Sheet (CSS)
SSIS Packages for SQL Server	Microsoft C#
Software Lifecycle Management	Agile Programming methodology
Unified Logging Service (ULS)	Data Form Web Part Development
Microsoft SQL Server	Structured Query Language
Proficiency in use of these items are required:	
Microsoft Office Suite	Adobe Flash
Microsoft Server Operating System	Microsoft SharePoint Workflows
Microsoft Internet Information Services (IIS)	Adobe Design Suite

Microsoft SharePoint development	Oracle registry settings
Data Warehouse/Data cube concepts	

4.11.7.2 Application Program Development and Analysis

- Support, develop, and maintain Keyport applications.
  - Estimate 30 web-based applications
- Provide troubleshooting support for reported bugs on Corporate Applications
- New development must meet Government defined standard and requirements. All projects shall be deployed with NO major bugs, and no more than 10 minor bugs.
- Newly developed and enhanced applications shall be delivered as fully tested and operational and shall conform to the operational environment and specified user requirements prior to release
- Provide system design documents that are in accordance with approved government defined processes and guidelines
- Conversion projects shall provide parallel processing and/or system validation of the old and new systems prior to implementation
- There are 3 different levels of complexity in the development environment
  - High Level Complexity projects – Throughout the life of the contract there will be a consistent workflow of 2 active projects. High level complexity is distributed computing with ground up development; hand crafted to customer requirements, involving database development (design of tables, indexes, stored procedures, functions, views, etc.), custom code developed using .NET 3.5 and above
  - Mid-Level Complexity projects – Throughout the life of the contract there will be a consistent workflow of 3 active projects. Mid-level complexity is significant customization to an out of box solution with custom code and data manipulation
  - Low-Level Complexity - Throughout the life of the contract there will be a consistent workflow of 1 active project. Low-level complexity is minimal customization to out of the box solutions

4.11.7.3 Training Support

The contractor shall provide training support associated with system implementation, including detailed functionality of software modules, classroom exercises given in either formal classroom training, and/or one-on-one sessions as required. Training shall be performed for the organization in various configurations such as an all hands notice to users, to groups (i.e. sponsors, teams), and one-on-one. The Training Plan shall detail functionality of software modules. It shall contain exercises for participants to follow in a written format as well as a format suitable for overhead projection.

4.11.7.4 Post Implementation Support

The contractor shall provide support required after implementation, which includes responding to Helpdesk (trouble) requests for bugs and minor modifications reported or as assigned by the government.

4.11.7.5 Quality Control

The contractor shall provide thorough Quality Assurance (QA) testing of all new and modified application systems to preclude failures in a production environment. This includes all applications developed by contractor or Government. General testing includes the following test plans:

- Developer Test Plan
- QA Test Plan
- Underlying Data Test Plan
- Beta (User) Test Plan
- Beta (User) Test Plan using Software Test Plan
- Conduct QA testing and provide written documentation of results.
- Reporting Requirements - Where no Government format is provided, contractor format is acceptable

4.11.7.6 Computer System Analyst Support

The contractor shall provide the following support for Corporate Application Team Projects:

- Research routine user problems and report to the Government for disposition
- Recommend modifications to established processes/practices to streamline development standards
- Monitor compliance with processes and quality relating to industry standard software development processes

- Audit software products and report/track any non-compliance issues
- Prepare reports/metrics from specified applications

4.11.8 IT Asset Management

- Support IT asset management activities in accordance with applicable IC and DoD policies, instructions, and guidance.
- Make recommendations to improve IT asset management processes and procedures in accordance with IC and DoD policies, instructions, and guidance.
- Perform IT asset management activities to support the processes of inventory, IT receiving, re-use, and disposal.
- Produce written reports, presentations or other artifacts as required by the Government for each task assigned.
- Support activities to implement automated processes within the IT service management tool and configuration management database (CMDB).
- Support the development of IT asset management metrics.

4.11.9 Hardware/Software Management Support

Hardware and Software Procurement Support is a function performed within the IT Division for all NUWC Keyport Codes. Contractor tasking will include:

- Working with various Keyport customers on IT procurement actions
- Process ITPRs submissions, in accordance with current FY guidance, within 5 working days of receipt
  - Estimate 35 ITRPs per month
- Process Department of the Navy (DON) Applications and DADMS new adds, associations, and updates
  - Estimate 60 actions per month
- Prepare Purchase Requisitions (PRs)
  - Estimate 50 actions per month
- Receipt material
- Track software licenses
- Ensure IT procurement items align with and are accounted for in the IT Budget
- Track software/hardware maintenance and work with customers to initiate maintenance renewals
- Maintenance renewals will occur NLT 3 months prior to expiration
- 100% of all maintenance renewals are processed on time
- Work with asset management for barcoding and tracking of IT equipment
- Provide monthly reporting on:
  - Number of request processed
  - Total time from customer request to acquisition process
  - ITPR process time
  - Upcoming maintenance contract renewals

4.11.10 Telecommunications Management

Telecommunications Management consists of the operation, ordering, delivery, and cancellation of data circuits, voice circuits, and wireless services. Specific tasking includes:

- Order, deliver, and cancel data and voice circuits via the DISA Direct Order Entry Process
- Order, deliver, and cancel voice services via Navy Communication Telecommunications Station, Bangor including Direct Inward Dialing (DID) numbers for VoIP services
- Order, receive, and deliver telecommunications equipment including analog phone equipment, VoIP phone equipment, cellular phones, pagers, satellite phones, air-cards, and associated peripherals
- Maintain a loan pool of GFE cellular equipment for temporary use
- Work on behalf of the Keyport customer to provide circuit one-time and recurring cost estimates and installation estimates
- Operate in alignment to Keyport directives 2300.1 and 2300.2 and higher level guidance
- Provide monthly metrics and trend analysis on the following:
  - DDOE request and type processed
  - Number of deployed cellular devices
  - Cellular devices with zero usage, over usage, and under-utilization
- Maintain cellular and analog equipment inventories in the government approved system

- Acknowledge customer requests within 30 minutes of receipt

4.11.11 Technical Writer/Documentation Support
Provide documentation support for creation and modification of project planning, policy, process, auditing, and review documents covering all Corporate IT Support tasking.

Estimate 12 document actions per week.

4.11.12 IT Drawing Support

- Provide technical drawing support for corporate IT infrastructures, to include but not limited to:
  - Network engineering drawings
  - Accreditation package drawings
  - Rack elevation drawings
  - Conceptual project drawings
  - As-built drawings
- Drawings will typically be completed in Microsoft Visio and or other Computer Aided Design (CAD) software
- For scoping purposes, estimate maintaining 300 – 500 drawings and 50 new drawing per year.
- Provide monthly metrics on number of drawings in queue, in-process, and completed
- Provide a nominal turnaround time of 5 working days for new drawings

4.11.13 IT Configuration Management

- Provide IT Configuration Management (CM) oversight for all Corporate IT Support tasking and RDT&E approved laboratories
  - Estimate 30 CM requests weekly
- Develop, modify CM workflows and sub tasks
- Manage CM Database (CMDB)
- Ensure CM SLA are met
  - Significant: 2 calendar days or less
  - Major: 14 calendar days or less
  - Minor: 30 calendar days or less
  - Routine: 1 calendar day
- Modify and maintain overall Corporate/RDT&E CM process
- Train users on CM tool
- Recommend strategies for CM improvements/faster processing times

4.11.14 Comptroller Process Automation Support
The contractor shall provide support to the Comptroller Department (Code 01) which includes automated processes and local reports using lifecycle management techniques, including:

- Planning for Future Requirements
- POA&Ms
- Specifications, Design, Development, Testing and Acceptance, Deployment, and Maintenance.
- Provide documentation of current automated processes and local reports.

Responsibilities include:

- Plan and assist in the execution of regularly scheduled production job streams supporting local Management Information Systems (MIS).
- Respond to daily IT Support Tickets regarding programs or job streams and reports that fail to execute properly based on the level of urgency. (IT Support Tickets urgency is predetermined by the production schedule).
- Assist in incorporating new releases of MIS.
- Provide support for Comptroller Department data calls.
- Enhance or develop reports or processes in support of automation initiatives and emerging requirements. Document processes using Visio.
- Provide all software/scripting packages for operating new or enhanced programs, forms or reports. Maintain and update documentation including the interfaces for existing Comptroller automated processes currently in Access, Visual Basic, MS

Office, SharePoint, or SQL Server. Support development of forms using INFOPATH.

- Provide ongoing support for the maintenance of current and historical financial data in ERP and other systems with financial data. The support shall include:
- Develop reports
- Participate in meetings, phone calls, and training
- Provide data from existing systems upon request
- Review system documentation upon request (Functional design specifications, data mapping, data conversion plans, etc.)
- Participate in VTC training
- Participate in verifying/testing data accuracy.
- Participate in design and planning events for retention of historical financial data and the maintenance of historical financial systems
- Maintain historical data and financial systems as required
- Document historical financial systems and processes
- Provide support for the Comptroller SharePoint site. The support shall include, but not be limited to:
- Upgrade and maintenance of the Comptroller SharePoint site.
- Assist in any upgrades to the SharePoint site
- Build/develop/design new features of SharePoint and propose implementation of those features beneficial to the Comptroller Department users.

4.11.15 Travel

Travel will be required in support of this effort as reflected in paragraph 4.14. All travel will be directed by the COR through TI's.

4.12 Task 12: Code 20 Cyber Security/Cyber Operations (CS/CO) Engineering Support

The CS functions are for various programs and projects internal and external to NUWC Keyport. These functions include preparing system accreditation documentation required by the Navy and/or DoD, evaluating security configurations of systems, and maintaining security configurations of production, development and test systems by applying and configuring security controls. The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.12.1 CS Support: System Security Configuration and Maintenance

For estimation purposes, assume full responsibility for maintaining the security configuration of a web-based production system running in an Oracle Real Application Cluster environment consisting of five database servers, and three application servers. Security configuration is to be maintained by the processing of IAVA's, STIG's and Critical Patch Updates, and the corresponding modification of system settings in the production environment.

4.12.2 CS Support: System Accreditation

For estimation purposes, assume responsibility for end-to-end preparation of a system accreditation package (System Accreditation Documentation) in accordance with the DoD Risk Management Framework requirements. Tasking includes assessing a windows-based system for compliance with DISA STIG's, completion of vulnerability scans and preparation of required supporting documentation. System to be accredited is comprised of a Tomcat application server, Microsoft SQL Server and Windows 7 client workstations.

4.12.3 CO Support: Software Vulnerability Assessment

For estimation purposes, assume responsibility to comprehensively analyze developed and procured JAVA and other software code in stand-alone, embedded and combat system applications for security vulnerabilities—with or without automated tools. Conduct penetration testing of JAVA and other software code in stand-alone, embedded and combat system applications software with or without automated tools. Assume 4000 hours of effort for each year of the contract.

4.12.4 Travel

No travel required.

4.13 Task 13: Augmented Reality/Virtual Reality

Augmented Reality (AR) and Virtual Reality (VR) current and future projects involve more than one fleet customer. Projects provide one or more services involving applied research and development of physical/functional new capabilities to a technical baseline, VR simulations for various training / non-training applications / devices and future augmented reality (AR) tools and content for operations and maintenance rehearsal of procedures. VR simulations are visually realistic and provide sailors with a highly immersive system-level training and on-the-job experience that can be easily accessed from school houses, shore facilities,

and while underway. A single system user interface using gestural / voice / eye-track navigation provides an access point to multiple simulations comprising a variety of learning, performance support, technical references and assessment content. Systems are flexible and easily expandable so that other types of simulations and performance aids can be integrated in the future along with future systems. The simulations utilize authoritative source data for technical narrative / text, 3D models, textures, and audio whenever possible. Data linkages are maintained between authoritative source data and any optimized or derived versions of the authoritative assets used in the simulation. The AR-VR team provides system design, applied research and prototype development, AR/VR solution design, usability engineering, product development, testing, implementation and support activities for current and future fleet customer projects, as well as providing government technical oversight.

SYSTEM ARCHITECTURE(S) / SOFTWARE TECHNOLOGIES	CURRENT DEPLOYMENT / UTILIZATION
SYSTEM ARCHITECTURES: AR and VR applications may be non-networked (standalone), or networked and fully integrated products hosted on program of record application systems on program of record LANs. Research and development network is rapidly reconfigurable to support various current and planned efforts. HARDWARE TECHNOLOGIES: The AR-VR delivery system features a Head-Mounted Display (HMD) with compatible hand held controllers or future controller technologies, linked either to an a) networked server, or b) a wearable standalone PC running the pre-installed Windows 10 and Unity software application suite and virtual technical content. The delivery systems are hardware agnostic and can be easily configured to run on various hardware configurations. SOFTWARE TECHNOLOGIES: C#, C++, Python, Unity, Jira, Bolt, 3D Studio Max, Maya, ZBrush, or Blender, Photoshop and Substance Painter.	Current project(s) are just beginning to deploy to multiple ashore and shipboard locations.

For AR-VR project(s), perform the functions in paragraph 4.13.1 The Government estimate of labor categories and cumulative hours required is in Attachment 03.

4.13.1 Augmented Reality/Virtual Reality Development and Enhancements

For estimation purposes assume two 3D Virtual Reality Artists and two Mixed Reality Software engineers required to support one new Augmented Reality/Virtual Reality development project per year, or two Augmented Reality/Virtual Reality enhancement projects to existing Augmented Reality/Virtual Reality applications per year. The actual number of projects to be assigned will be impacted by tasking and project complexity; tasking to complex and lengthy projects will reduce the number of different tasks assigned.

4.13.2 Travel

No travel required.

4.14 Travel

Travel will be required in support of this PWS as reflected in Attachment 05 Estimated ODCs (Travel/Material). All travel must be approved in advance by the COR via issuance of a TI which will include: identifying purpose, dates, and locations of travel. All travel must be in accordance with the Joint Travel Regulations (JTR). Any travel costs exceeding those allowed under JTR will not be reimbursed.

5.0 REPORTING REQUIREMENTS

Deliverables and reports relating to specific projects delivered by the Contractor to the Government under this contract shall prominently show the contract and task order number on the cover of the report.

5.1 Daily Reporting

The contractor shall communicate daily with the government project leads on the efforts regarding any issues that have arisen that have the potential to affect agreed upon delivery or accomplishment dates. These communications will be in person, or via phone and email. Holidays and weekends will normally be excluded from this requirement.

5.2 Recurring Reports

Distribution Statement D (DoD and DoD Contractors Only) applies to the reports under this paragraph.

5.2.1 Performance Status Report (CDRL A002)
A Performance Status Report will be submitted to the Government monthly in a written format of the contractor's choosing. Performance Status Reports will be sent to the COR and the Contracting Officer. The reports shall, at a minimum, contain the following for all work on the task order:

- A summary of all work done
- Compliance with established schedules, including work accomplished with sufficient detail to permit early identification of potential problems or schedule slippages
- Progress towards key events and milestones
- Problems encountered
- Significant personnel changes encountered or anticipated

5.2.2 Weekly Expenditures Report (CDRL A003)
A weekly expenditure report will be submitted to the COR starting no later than eleven (11) days after commencement of work on the task order and by the Thursday of each week thereafter for the previous week. The report shall contain the following elements:

Element 1: Cost Summary including funds depletion estimates based on efforts during the reporting period by funded CLIN, Project, and PWS functional area
Element 2: CLIN Ceiling, funded amount, Total funds expended, Average Weekly Spend Rate, Depletion Date, and Estimate at Completion (EAC) of the current task order period of performance.
Element 3: The report will also indicate when CLIN and Project will be 75% expended in accordance with FAR 52.232-20 Limitation of Cost or FAR 52.232-22 Limitation of Funds as applicable.

5.2.3 Cost Status Report (CDRL A004)
A Cost Status Report reflecting the expenditure of funds and man-hours will be submitted to the Government monthly in a written format of the contractor's choosing. The report will provide cost by contract paragraph. The report may be more frequent if the contractor's existing reporting system makes that periodicity more cost effective. Reports will be sent to the COR and the Contracting Officer. The reports shall contain the following for all work on the task order:

- Actual monthly fund expenditures, balances remaining and estimated funds depletion date, by individual paragraph effort
- Actual man-hour expenditures by individual paragraph effort

5.2.4 Electronic Cost Reporting and Financial Tracking (eCRAFT) (CDRL A005)
IAW contract clause C.124, the contractor shall submit required reports on the same day and for the same timeframe the contractor submits an invoice in the Invoice, Receipt, Acceptance, and Property Transfer (iRAPT) system (CDRL A005). The amounts shall be the same. eCRAFT acceptance/rejection will be indicated by e-mail notification from eCRAFT.

5.3 Single Submission Reports

5.3.1 Management Plan (CDRL A001)

A management plan describing the contractor’s organization, assignment of functions, duties and responsibilities, management procedures and policies and reporting requirements will be submitted 30 days after award. The plan shall be resubmitted if the plan changes.

5.4 Technical Documents and Reports / Contract Data Requirements List (CDRL)
Each of the Data Item Descriptions (DID) for these documents and reports has been tailored accordingly in its respective CDRL. Inspection and acceptance of these documents by the government will be in accordance with the Integrated Product Team procedures utilized; no formal transmittal document or other transmittal form will be required from the contractor. Contractor may request government acknowledge receipt via email. Distribution Code D (DoD and DoD Contractors Only) applies to CDRLs A001-A005.

Table C6-CDRLs

CDRL	Data Item Description	Formal DID Title	PWS Document Title

	(DID) ID		
A001	DI-MGMT-80004A	Management Plan	Management Plan
A002	DI-FNCL-80912A	Performance and Cost Report	Performance Status Report
A003	DI-MGMT-80227	Progress, Status and Management Report	Weekly Expenditure report
A004	DI-FNCL-80331A	Funds and Man-Hours Expenditure Report	Cost Status Report
A005	DI-MGMT-81991	Contract Status Report	eCRAFT

6.0 GOVERNMENT FURNISHED PROPERTY

6.1 Accounting Records

Government property that is determined to require accounting records to ensure accurate custody trails (e.g. laptop computers, tablet computers, smart phones etc.) will be transferred to the contractor on a DD1149, Requisition and Invoice/Shipping Document. The assignment of standard office equipment such as desktop computers, networked printers and desktop monitors will not be transferred to the contractor's custody, but will be made available for contractor use within government offices and facilities. The custody of other government property may be transferred to enable contractor work, but none is envisioned at this time.

6.2 Computers

The Government will provide NMCI computers for the use of the Contractor in performing the requirements of the PWS.

The Contractor shall comply with the following guidelines:

a. Connection of privately owned computers to a Government network is prohibited.

b. Connection of privately owned handheld computing devices to Government computers and networks is prohibited.

c. Use of privately owned software on Government computers is prohibited.

Telework may be approved on a situational basis during the period of performance of the contract. If telework is required and a contractor needs to take government property off station, the contractor will follow the requirements of the government furnished property clauses in the contract.